

**DIGITAL WATERMARKING IN 2D AND 3D
TRANSFORM DOMAINS FOCUSING ON FIDELITY
AND ROBUSTNESS**

ALMAS ABBASI

**THESIS SUBMITTED IN FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY**

**FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2014

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **ALMAS ABBASI**

Registration/Matric No: **WHA110006**

Name of Degree: **DOCTOR OF PHILOSOPHY**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

Digital Watermarking in 2D and 3D Transform Domains Focusing on Fidelity and Robustness

Field of Study: **DIGITAL WATERMARKING**

I do solemnly and sincerely declare that:

- (1) I am the sole author/writer of this Work;
- (2) This Work is original;
- (3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
- (4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
- (5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
- (6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature

Date:

Subscribed and solemnly declared before,

Witness's Signature

Date:

Name:

Designation:

ABSTRACT

Digital watermarking technique has been used to deal with issues like copyright protection and authentication to protect legitimate right of the owner and prevent illicit attempt to supersede it by the adversaries. These issues have become a matter of concern due to pervasive usage of digital media at various platforms in recent years. Robust watermarking techniques are usually applied for copyright protection, content authentication and temper localization because it can resist various kinds of manipulations on it. There is a need of developing a truly robust watermark to handle complicated and complex attacks. In this thesis, we focus on geometrically robust watermarking techniques especially invariant domain based technique for digital images. Additionally, we also studied schemes for three dimensional (3D) image representation named Depth Image Based Rendering (DIBR).

We have proposed a robust dynamic block based watermarking technique in 2D domain using Genetic Programming (GP) to achieve imperceptibility and robustness. This technique can embed an imperceptible and robust watermark in images irrespective of the size of the blocks. We present a GP based perceptual shaping function which determines the optimal watermark strength for the selected coefficients using Human Visual System characteristics (HVS) such as luminance sensitivity, and self and neighborhood contrast masking. Our proposed scheme can resist image processing attack, noise attack, geometric attack and cascading attack. Comparison results show that our dynamic block based technique is approximately 5% and 23% more robust than the other two compared techniques.

In addition, we proposed two new invariant domain based watermarking techniques. They are Rotation, Scaling and Translation (RST) invariant domain based on Riesz

Transformation (RT), and fractional calculus based polynomial watermarking domain. We are the first to explore invariant properties of RT, fractional sinc and fractional Heaviside function. The advantage of invariant domain based watermarking techniques is they do not need resynchronization step for the watermark detection. It results in less processing time, and less distortion induced due to resynchronization process.

We also extended watermarking from two dimension (2D) environment to 3D scenario. We have proposed an imperceptible and robust watermarking scheme in Multi-Dimensional Wavelet Transformation (MDWT) domain for the content protection of 3D DIBR. Interval Type-2 Fuzzy Logic System (IT2FLS) is used to determine the weight factor using noise visibility and entropy value to embed watermark imperceptibly. The proposed technique embeds watermark with least distortion in the rendered left and rendered right images for imperceptibility. The experimental results show that the proposed technique is robust against JPEG compression, depth image alteration, Gaussian noise and rotation attacks. Moreover, the bit error rate (BER) of the extracted watermark is nearly negligible.

ABSTRAK

Teknik Watermarking digital telah digunakan untuk menangani isu-isu seperti perlindungan hakcipta dan pengesahan untuk melindungi hak sah pemilik dan mencegah percubaan haram untuk menggantikannya oleh musuh. Isu-isu ini telah menjadi perkara yang membimbangkan disebabkan oleh penggunaan meluas media digital dalam pelbagai platform pada tahun-tahun kebelakangan ini. Teknik Watermarking mantap biasanya digunakan untuk perlindungan hakcipta, pengesahan kandungan dan penyetempatan perubahan kerana ia dapat menahan pelbagai jenis manipulasi ke atasnya. Terdapat keperluan membangunkan watermark yang benar-benar mantap untuk mengendalikan serangan rumit dan kompleks. Sebagai tambahan, satu domain watermarking tak berubah baru diperlukan. Dalam tesis ini, kami memberi tumpuan kepada teknik watermarking geometri mantap terutamanya teknik berasaskan domain tak berubah untuk imej digital. Selain itu, kami juga mengkaji skim perwakilan tiga dimensi (3D) yang dinamakan Rendering Imej Berdasarkan Kedalaman imej (DIBR).

Kami telah mencadangkan satu teknik watermarking multiblok teguh berpangkalan di domain 2D menggunakan Pengaturcaraan Genetik (GP) untuk mengimbangi imperceptibility dan keteguhan. Teknik ini boleh memasukkan satu watermark tak kelihatan dan teguh dalam imej tanpa mengira saiz blok. Kami membentangkan fungsi membentuk persepsi berasaskan GP yang menentukan kekuatan watermarking optimum bagi pekali yang dipilih dengan menggunakan ciri-ciri Sistem Visual Manusia (HVS) seperti sensitiviti lumina dan kejiranan masking kontras diri dan jiran. Skim yang kami cadangkan boleh menentang serangan pemprosesan imej, serangan bunyi, serangan geometri dan serangan melata. Perbandingan keputusan menunjukkan bahawa teknik

berasaskan multiblock kami adalah lebih kurang 5% dan 23% lebih kukuh daripada dua teknik lain yang dibandingkan.

Selain itu, kami mencadangkan dua teknik watermarking berasaskan domain tak berubah baru. Mereka adalah domain tak berubah terhadap Putaran, Skalaan dan Terjemahan (RST) yang berdasarkan Transformasi Riesz (RT) dan domain berasaskan kalkulus pecahan polinomial. Kami adalah yang pertama dalam meneroka sifat-sifat tak berubah bagi RT, sinc pecahan dan fungsi Heaviside pecahan. Kelebihan teknik watermarking berasaskan domain tak berubah adalah mereka tidak perlu langkah penyerentakan semula untuk mengesan watermark. Ia mengurangkan masa pemprosesan dan mengurangkan gangguan akibat proses penyerentakan semula.

Kami juga melanjutkan watermarking dua dimensi (2D) ke persekitaran senario 3D. Kami telah mencadangkan skim watermarking tak kelihatan dan teguh dalam domain Transformasi Wavelet Multi Dimensi (MDWT) untuk perlindungan kandungan 3D DIBR. Sistem Logik Kabur Selangan Jenis-2 (IT2FLS) digunakan untuk menentukan faktor pemberat dengan menggunakan penglihatan bunyi dan nilai entropi untuk menanamkan watermark secara tak kelihatan. Teknik yang dicadangkan menanamkan watermark dengan penyelewengan kurang dalam imej kiri dan imej kanan untuk imperceptibility. Keputusan eksperimen menunjukkan bahawa teknik yang dicadangkan adalah teguh terhadap pemampatan JPEG, perubahan kedalaman imej, bunyi Gaussian dan serangan putaran. Selain itu, kadar ralat bit (BER) dalam watermark yang diekstrak adalah hampir boleh diabaikan.

ACKNOWLEDGEMENTS

First of all I thank almighty ALLAH for the courage and patience given to me to complete this research work in stipulated time frame.

I would like to thank my supervisor Dr. Woo Chaw Seng, from whom I learnt a lot, and enjoy my work. I really thank him and am grateful to him for his encouragement, support and direction during my research.

I wish to thank and acknowledge Dr. Rabha Wael Ibrahim, Dr. Imran shafiq Ahmad, Dr. Asia sultan, and owe a lot to them, for their timely support, valuable suggestion and discussion during this study.

I am deeply thankful to my family, specially my parents for their unconditional support, constant encouragement, prayers, and understanding. They have been my source of strength throughout.

Finally i am indebted to the University of Malaya (UM) for the award of Bright Spark Scholarship, which provided me the opportunity to carry out my PhD here. It was great experience for me. Thank you very much I really enjoyed working here.

Almas Abbasi,

September, 2014.

TABLE OF CONTENTS

Original Literary Work Declaration Form	ii
Abstract	iii
<i>Abstrak</i>	v
Acknowledgements	vii
Table of Contents	viii
List of Figures	xiii
List of Tables	xvii
List of Symbols and Abbreviations	xix
CHAPTER 1: INTRODUCTION.....	1
1.1 Background	1
1.2 Research Motivation	2
1.3 Problem Statement	3
1.4 Research Questions	3
1.5 Research Aims and Objectives	4
1.6 Expected Contributions	4
1.7 Research Scope	5
1.3 Organization of the Thesis	6

CHAPTER 2: LITERATURE REVIEW.....	8
2.1 Digital Image watermarking	8
2.1.1 Digital watermarking	8
2.1.2 Digital watermark properties	8
2.1.3 Watermark domains	11
2.1.4 Watermarking applications	12
2.1.5 Attacks category and their countermeasure	12
2.1.6 Blind watermark detection	14
2.2 Properties of Human Visual System/ Perceptual modelling of a digital watermark..	14
2.2.1 Luminance	15
2.2.2 Contrast	16
2.2.3 Entropy	17
2.2.4 NVF	19
2.2.5 Watson perceptual model	21
2.3 Perceptual Modelling using AI techniques	24
2.3.1 Genetic Programming	24
2.3.2 Typical representation of a genetic program	25
2.3.3 A basic GP algorithm	26
2.3.4 Perceptual model based watermarking techniques	28
2.3.5 Fuzzy logic	31
2.4 RST Invariant Domain	33
2.4.1 Robust image watermarking and RST attacks	33
2.4.2 Watermarking techniques using RST invariant domain	34

2.4.3 Riesz Transformation	37
2.4.4 Watermarking techniques in polynomial transform domain	38
2.5 Watermarking techniques using 3D image representation DIBR	47
2.5.1 Multi-dimensional discrete wavelet transforms	49
2.5.2 Related work	49
2.6 Chapter Summary	51

CHAPTER 3: GENETIC PROGRAMMING FOR PERCEPTUAL MODELLING

WITH DYNAMIC BLOCK SIZE 53

3.1 Methodology	53
3.2 Human Visual System (HVS)	56
3.3 Experimental Results Discussion	59
3.3.1 Filtering Attack	63
3.3.2 Noise Attack	65
3.3.3 Compression Attack	65
3.3.4 Cascading Attacks.....	66
3.3.5 Geometric Attacks	66
3.4 Chapter Summary	67

CHAPTER 4: INVARIANT DOMAIN WATERMARKING USING RIESZ

TRANSFORMATION.....68

4.1 Methodology	69
4.1.1 Watermark Embedding	69
4.1.2 Watermark Detection	72

4.2 Experimental results discussion	73
4.2.1 Imperceptibility	74
4.2.2 Robustness	75
4.2.3 Comparison with Existing Methods	84
4.3 Chapter Summary	85

CHAPTER 5: INVARIANT DOMAIN WATERMARKING USING FRACTIONAL CALCULUS 86

5.1 Sinc Function	87
5.2 Heaviside Function	89
5.3 Methodology	92
5.3.1 Using FSC	92
5.3.2 Using HFOA	95
5.4 Experimental results and discussion using FSC	99
5.4.1 Imperceptibility	100
5.4.2 Robustness	101
5.5 Fractional Rotation matrix expression	104
5.6 Experiments results and discussion using HFOA	105
5.6.1 Imperceptibility	105
5.6.2 Robustness	106
5.7 Chapter Summary	110

CHAPTER 6: FUZZY LOGIC AND WAVELET TRANSFORM BASED WATERMARKING FOR 3D IMAGES 111

6.1 Initial study of wavelet based watermarking for 3D Images	111
---	-----

6.2 Multidimensional wavelet based watermarking for depth image based rendering	
3D images	115
6.3 Methodology	116
6.3.1 Watermark embedding and detection	117
6.3.2 Hole filling	120
6.4 Experimental Results and Discussion	121
6.4.1 JPEG Compression attack	122
6.4.2 Gaussian Noise Addition attack	122
6.4.3 Rotation attack	123
6.4.4 Comparison with existing techniques	125
6.5 Chapter Summary	126
CHAPTER 7: CONCLUSIONS	127
7.1 Achievement of the Objectives	128
7.2 Future Works	130
REFERENCES.....	131
PUBLICATIONS	141

List of Figures

Figure 2.1: Human Eye and its different parts	15
Figure 2.2: GP Simulation for evolving best candidate	27
Figure 2.3: GP search flow	28
Figure 2.4: Overview of IT2FLS	32
Figure 2.5: Depth image base rendering procedure	48
Figure 2.6: One-level 3D DWT structure	49
Figure 3.1: Dynamic block watermarking Technique flow diagram. Perceptual analysis part is performed by the GP	55
Figure 3.2: Comparison of imperceptibility of the proposed multi-block technique on different images with different block sizes	61
Figure 3.3: Comparison of PSNR and MSE values for the low pass filter attack on image using different block sizes	64
Figure 3.4: PSNR and MSE values for the median filtering attack of varying strength on images using different block sizes	64
Figure 3.5: Comparison of adding Gaussian noise with different variance, such as 0.5k, 1k, 5k, 10k, 15k on image using different block sizes	65
Figure 3.6: Comparison of JPEG attack of varying quality factors, together with Gaussian noise attack with different variance on images using different block sizes	66

Figure 4.1: Frequency responses (real / imaginary part) of the components filters of the first, second and third order Riesz transformation. The origin of the 2-D frequency domain is in the center and the intensity is stretched linearly for maximum contrast. (Unser & Van De Ville, 2010)	69
Figure 4.2: Overview of input and output of IT2FLS	71
Figure 4.3: Process flow of the proposed technique	72
Figure 4.4: Watermark detection for the invariant domain.....	73
Figure 4.5: Original (a-e) and watermarked test images (f-j).....	74
Figure 4.6: Robustness against RST attack at scale 2 of Riesz Transformation: Correlation in five test images: (a) Average correlation of five test images after scaling attack. (b) Average correlation of five test images after rotation attack. (c) Average correlation of five test images after translation attack zero with padding along y-axis. (d) Average correlation of five test images after translation attack zero with padding along x-axis	81
Figure 4.7: Robustness against rotation attack using LPM and RT of five test images	82
Figure 5.1: The Sinc Function	87
Figure 5.2: Heaviside step function	90
Figure 5.3: Watermark embedding scheme for the Invariant domain	93
Figure 5.4: Watermark Detection.....	94
Figure 5.5: (a-e) Original Test Images, (f-j) Watermarked Test Images	100
Figure 5.6: Robustness of Proposed Technique against different types of attacks. (a) Gaussian Noise. (b) JPEG Compression. (c) Aspect ratio attack. (d) Row Column removal attack. (e) Scaling attack. (f) Sharpening attack	101

Figure 5.7: Experimental results:(a) to (e) show the watermarked test images manipulated by using aspect ratio of 2:7 in relation to x and y axis; (f) to (j) represent watermarked images corrupted by using sharpening attack;(k) to (o) illustrate the watermarked images are compressed with JPEG compression attack with quality factor 50;(p) to (t) display the scaled down to 50% of the image size	103
Figure 5.8: (a-d) Rotation achieved using fractional rotation expression having angle 15, 25, 30 and 45 respectively	105
Figure 5.9: (a-e) Watermark test images: Random bending attack with wrap factor value changes from 2 to 4.	107
Figure 5.10: (a-e) Original Test Images, (f-j) Attacked watermarked Test Images: Rotation attack for different values of the angels are taken as 5,10,15,30 and 45 respectively.....	107
Figure 5.11: Robustness against scaling and circular shift Attack: (a) Comparison of the Correlation and Threshold values of five watermarked test images against the circular shift attack. (b-f) Comparison of Correlation values of five images after scaling attack of the proposed technique.....	108
Figure 5.12: Robustness of Proposed Technique against Rotation attacks. Five standard images are tested for the rotation attack. Rotation angle is taken of different values such as 5, 10, 15, 30, 45 degrees.....	109
Figure 6.1: Overview of IT2FLS inputs and output for the proposed scheme	116
Figure 6.2: Proposed watermarking Embedding Scheme.	119

Figure 6.3: Watermark detection in the proposed scheme.....	120
Figure 6.4: 3D original center images and depth images.....	121
Figure 6.5(a): Comparison of PSNR and MSE values of five standard watermarked images using constant weight factor and the weight factor determined using IT2FLS respectively.	123
Figure 6.5(b): Comparison of PSNR values of watermarked Book images after the Gaussian Noise and JPEG compression attack respectively.....	124
Figure 6.5(c): Comparison of PSNR values of watermarked depth image of Doll after the JPEG compression and Gaussian Noise addition attack.....	124
Figure 6.5(d): Comparison of PSNR values of watermarked Moeibus and Doll images after the JPEG compression and Gaussian Noise addition attack respectively...	124
Figure 6.6: Rotation and Gaussian noise attack effect on different 3D watermarked center images.....	125

List of Tables

Table 2.1 : Watermarking Attack Classifications	13
Table 2.2 : Basic function $A\lambda\theta$ amplitude for 6-level 1st level for a 9/7 dwt	23
Table 2.3 : Parameters for DWT threshold model	23
Table 3.1 : Basic function amplitude for 1st level for a 9/7 dwt (Liu et al.,2006)	58
Table 3.2 : Parameters for DWT threshold model (Liu et al., 2006).	58
Table 3.3 : GP control parameters.....	60
Table 3.4 : Comparison of cascading attack of varying strength, on image using different block sizes.	62
Table 4.1 : PSNR and SSIM value of watermarked images at second level of RT.	75
Table 4.2 : Performance of the proposed technique at second orders first, second and third scale of RT.....	76
Table 4.3 : Performance of the proposed technique and comparison of robustness test with other techniques.	83
Table 5.1 : PSNR and SSIM value of sample test images in the proposed FSC Domain.....	100
Table 5.2 : PSNR and SSIM value of sample test images in the proposed HFOA Domain.....	106
Table 6.1 : PSNR, MSE and BER values of watermarked center testing Images.	112
Table 6.2 : PSNR, MSE and BER values of Watermark Center Image after applying Gaussian Noise Attack of Different Variance Such As 50, 100, 150, 200.	113

Table 6.3 : PSNR, MSE and BER values of Watermark Center Image after Applying JPEG
Compression Attack of Different Quality Factors such as 50, 60, 70, 80, 90, 100.

.....114

Table 6.4 : PSNR, MSE values of Watermarked center image show the watermark
detection in the rendered right image with calculated bit error rate.121

University of Malaya

List of Symbols and Abbreviations

2D	:	Two Dimensional
3D	:	Three Dimensional
AI	:	Artificial Intelligence
BER	:	Bit Error Rate
DCT	:	Discrete Cosine Transformation
DIBR	:	Depth Image Based Rendering
DWT	:	Discrete Wavelet Transformation
FSC	:	Fractional order of Sinc
GP	:	Genetic Programming
HFOA	:	Heaviside Fractional Order of Alpha
HVS	:	Human Visual System
IT2FLS	:	Interval Type 2 Fuzzy Logic System
JND	:	Just Noticeable Distortion
LPM	:	Log Polar Mapping
MDWT	:	Multidimensional Wavelet Transform
MSE	:	Mean Square Error
NVF	:	Noise Visibility Function
PSNR	:	Peak Signal_to_Noise Ratio
RST	:	Rotation Scaling Translation
RT	:	Riesz Transformation
SSIM	:	Structure Similarity Index Measure

CHAPTER 1: INTRODUCTION

1.1 Background

The widespread use of social media sites such as Facebook and twitter, for sharing and exchanging of digital data makes it challenging to maintain copyright and proprietorship of data. Digital watermark is data or information which is embedded into digital image to uniquely identify it. Digital watermarking is a technique used to hide data/ information in images in such a way that it is invisible to users. Digital watermarking techniques have been used to deal with issues like copyright protection and authentication to protect legitimate right of the owner and prevent illicit attempt to supersede it by the adversaries. These issues have become a matter of concern due to pervasive usage of digital media at various platforms in recent years. Two important issues should be considered. Firstly, there is a need of developing a truly robust watermark domain to handle complicated/complex attacks Secondly, imperceptible watermark techniques are required.

The idea of watermarking can be traced back with the concept of paper watermark in 1282, Italy. Thin wires in different directions were added to paper mould as watermark. Shaded watermark was first used in 1848. Till the 18th century the watermark were primarily used on postage stamps, documents and on money as anti-counterfeiting measure. More prominent and advance watermarking techniques were proposed in nineteen century to protect the digital contents.

Digital watermarking can be divided into 3 broad categories (Pan, Huang, & Jain, 2004). These are robust, semi fragile and fragile watermarking. Robust watermarking are those in which it is assumed that the watermark is resistant to intended and unintentional attack such as rotation, scaling, cropping, translation and compression. On the other hand semi fragile watermarking and fragile watermarking refer to those scenario, where the

watermark is used for content authentication. Watermark is easily destroyed when any modification or tempering is performed on the associated digital content.

Digital watermarking is a tool that enables content protection through obscure information embedding. Cryptography provides means to protect the contents of data using encoded techniques. However, cryptography provides no protection once the content are decrypted, whereas watermark remains hidden and embedded in the content even after the contents are decrypted thus providing further protection. Watermarking technique inserts a signal into the image without disturbing its visual quality. Then, the watermark image is made public or sent to the end user. Later the identified watermark is used for the purpose of copyright protection and content authentication.

1.2 Research Motivation

Social media such as Facebook and twitter seems to grow at the speed of light. “Facebook users uploaded more than 250 billion photos to the site and currently average 350 million upload per day”. “ On a busy day, twitter gets about 170 million tweets, 1.25% means 2.125 million tweets daily links to pictures from a third party services”(Grove, 2011).

Images like digital arts, paintings in digitized form, cultural heritage painting in digitized form, illustrative diagrams and digital photographs are the basics of multimedia contents.

With development in computing software and hardware, digital contents are prone to attacks and need copyright protection. For example, images can be distorted by copying and modification. The modified contents can be distributed easily. Digital watermarking offers a method for authentication and copyright protection.

The performance and application of digital watermarking are influenced by watermark robustness, this denotes the potential of watermark to withstand common image processing attack. Digital watermarking techniques have been proposed in the past but designing a robust image watermarking scheme is still a challenging task because different kind of attacks especially geometric attacks can displace a watermark which makes it impossible to detect the watermark. Moreover, watermark embedding requires imperceptibility so that images should be least distorted due to the watermark embedding.

1.3 Problem Statement

Robust watermarking techniques need to have balance with fidelity and allow extension from 2D to 3D domain.

1.4 Research Questions

To close the gap this research answers the following research questions:

1. What are the advantages of GP (Genetic Programming) in designing a Human Visual System (HVS) mask for imperceptible watermark?
2. Does Fuzzy Logic enable the balance between robustness and imperceptibility?
3. Can we obtain RST (Rotation Scaling and Translation) invariant using transformation operation?
4. Can polynomial transformation offer watermark invariant property?
5. How to extend 2D algorithm into 3D algorithm to achieve robustness and imperceptibility?

1.5 Research Aims and Objectives

The aims of this research mainly focus on the two important watermarking properties. These are robustness and imperceptibility of watermark in 2D and 3D Depth Image Based Rendering (DIBR) images.

To achieve the aims, the following objectives need to be accomplished.

1. To exploit the characteristics of HVS using GP to formulate a perceptual shaping expression for a dynamic block approach.
2. To exploit the characteristics of HVS using Interval Type-2 Fuzzy Logic System (IT2FLS) to calculate an appropriate watermark weight factor for each coefficient of the image to embed watermark imperceptibility.
3. To design /propose and evaluate a new invariant domain for watermarking.
4. To propose and evaluate a new polynomial transformation based invariant domain for watermarking.
5. To propose and evaluate a robust watermarking technique for 2D plus depth images /DIBR 3D images.

1.6 Expected Contributions

Following are the expected research contributions

- GP is an intelligent technique and has been used in different application for optimization purpose. This research work will proposed a dynamic block based robust watermarking technique in wavelet domain. GP will be used to evolve an optimized expression to embed watermark in images using different block sizes in wavelet domain.

- ITFLS based systems have been proposed in different areas successfully. This research will describe a HVS model based on IT2FLS to tackle the imperceptibility problem efficiently. Using this we will try to obtain best possible watermark weight factor value for each of pixels such that it keep optimum level of imperceptibility.
- Invariant domain for watermarking will be obtain using RT and polynomial transformation. Polynomial transformation based on fractional calculus will be introduce and will be used in watermarking. We will also introduce fractional Gaussian field based, fractional variance and threshold. Experimental results confirmed the resulting domain is rotation, translation and scaling invariant.
- We will also propose a 3D DIBR image based robust watermarking technique using Multidimensional wavelet transform and IT2FLS to take into account the robustness and imperceptibility properties of watermark. Watermark will be embedded in the center image and after wrapping operation the right image and left image will be checked for watermark.

1.7 Research Scope

To make sure that this research accomplish its set of objectives within the stated timeframe, the scope of this research is determined. In this thesis, we investigate two important properties of watermark i-e robustness and imperceptibility. Assuming capacity is fixed/constant so that we only need to balance the robustness and imperceptibility properties. Our focus is on invisible watermark as it causes less distortion to an image and preserve its original appearance/ originality. We prefer invariant domain because it needs less time and also there is no need to resynchronize using feature points.

Resynchronization induces distortion in the image which make it difficult to detect the watermark. Moreover we performed experiments on gray scale images to keep our attention on basic data embedding behavior. However, established watermarking schemes can also be used for the color images. Color display consist of red, green, and blue (RGB) components. Television broadcast mostly use YUV color model, where Y component represent the luminance, and U and V component represent chrominance components. Computer display uses RGB model. Therefore we can select the blue component of color image for our watermarking schemes as the distortion induced in this component is considered to be less sensitive for human eye.

1.8 Organization of the Thesis

This thesis comprises of seven chapters. Chapter 1 presents a brief background of study and its challenges. It also include research questions, research aim, objectives and scope of the research.

Chapter 2 review existing literature on 2D and 3D watermarking schemes and covers definitions of watermarking, its property, and applications and domains in which it has been applied commonly. Moreover this chapter also briefly describe different terminology, functions, models used in the study. Then existing approaches, are also discussed and elaborated. This chapter is in fact prelude, for further discussion of the rest of the chapters.

Chapter 3 is first among the 4 chapters, which describe the contribution/objectives of the thesis. It explore GP based watermarking technique in wavelet domain for dynamic block size. Experimental analysis, comparison, discussion and conclusion in the form of chapter summary is presented.

Chapter 4 describes methodology for Riesz Transformation (RT) based invariant domain techniques. It also includes RT and LPM (Log Polar Mapping) version of the technique. Detail of the experimental results, comparison with other techniques, discussion are presented for evaluation purpose. In the last conclusion is presented in the form of chapter summary.

Chapter 5 explores the fractional sinc and fractional Heaviside function properties for watermarking domain. In-depth experimental analysis and discussion are presented.

Chapter 6 describes a watermarking scheme for 3D DIBR images. Discussion and experimental results are given in details. Further comparison with other technique are made for evaluation purpose.

Chapter 7 concludes the research in the context of achievement of the research objectives, followed by future work directions.

CHAPTER 2: LITERATURE REVIEW

2.1 Digital Image Watermarking

The following section describe digital watermarking, digital watermarking properties, watermark domains, watermarking applications and watermarking attacks.

2.1.1 Digital watermarking

Receiving and transmitting digital data has prompted its widespread presence and storage. The technologies that cause this deluging of digital data are internet, compact disk read only memory CD ROM and DVD. The usage of digital data on a broader scale has brought a lot of convenience in different aspects, but it is not without side effects and issues raised such as tampering and copyright protection. With digital data so broadly used, watermarking are mostly used to address these issues. Watermarking is a method to embed a message while stenography is the art of hidden communication. The purpose of watermarking is to keep the message secret whereas data hiding is a general term and covers a vast range of problems related to making information confidential. (van der Veen, Lemma, Celik, & Katzenbeisser, 2007).

2.1.2 Digital watermark properties

In general watermarking techniques necessitate certain properties. These properties are required for all kinds of multimedia data such as audio, video and images. However, the significance of these properties varies with the purpose and application, of watermarking. In case of copyright protection the watermark should be robust enough to resist any attempt for its removal. While for the authentication applications, robustness is not required. The fundamental watermarking system properties are:

- **Imperceptibility**

Some aspects of a watermarking system need proper focusing. Imperceptibility is the most important amongst them. In a watermarking system a watermark must distort the cover image imperceptibly. Conceptually watermark must be invisible to naked eyes even with the help of highest quality equipment.

For a large number of the applications it is advantageous for the embedded mark to be invisible to the human eye. Attempts have been made to hide the watermark in such a way that it is not noticeable. However this constraint contradicts certain requirements such as robustness.

To estimate the imperceptibility of a watermark in a watermarking techniques researchers usually deployed Peak-Signal-to-Noise-Ratio (PSNR), Structure Similarity Index Measure (SSIM) (Z. Wang, Bovik, Sheikh, & Simoncelli, 2004), Mean Square Error (MSE) metric. SSIM uses the assumptions that HVS is highly adopted for extracting structural information using local pattern of pixel intensities based on luminance and contrast values. These reliance make information available about the configuration of the object in an image, which are ignored by the error based procedures. PSNR is measured using equation 2.1 below,

$$PSNR = 10 \log_{10} \left(\frac{(I_{MAX})^2}{MSE} \right) \quad 2.1$$

where I_{MAX} is the maximum gray levels of the image and it is equal to the value of 255. MSE denotes the mean square error represented by the following equation:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \left(I'(m,n) - I(m,n) \right)^2 \quad 2.2$$

Where $I'(m,n)$ is the watermarked image and $I(m,n)$ is the original image.

- **Robustness**

Before a watermark is retrieved from a watermark image, the watermark image could suffer certain attacks. An attack is described as any manipulation of watermark image that can impair the watermark. In the process of designing a watermark system, resistance against attacks is considered as a fundamental issue. Almost all watermarking methods are required to be resilient against any deliberate or accidental processing of image. This is usually called robustness. As different applications are confronting with different sets of plausible attacks, these attacks and their countermeasure are explored in the perspective of watermark applications. Therefore, while planning a watermarking system, its anticipated applications and related conceivable attacks need a higher degree of consideration.

Video signals, image and digital music usually have many distortions. Particularly in digital image case, these distortions include compression attack, filtering attack such as median filter attack etc, scaling, contrast enhancement, cropping, rotation, etc. Watermarking system is meant to keep the watermark detectable even after such distortions. If the watermark is embedded in perceptually a significant part of the signal, robustness against signal alteration can be attained effectively because visually important parts will not be attacked, modified easily. The same is the case with lossy compression procedures which remove perceptually irrelevant data. However the imperceptibility obligation of a watermark, pursues to encrypt information in extra bits that can be removed by compression operation. Usually geometric alteration or addition of noise may disable the watermark. For image watermarking to resist geometric alteration like rotation, scaling, translation, a lot needs to be done for copyright protection.

- **Robustness versus imperceptibility**

Robustness and imperceptibility have a key relationship with contradicting property of a watermarking system. If imperceptibility is improved robustness decreases. Therefore we want to strike a balance between these properties according to the domain of application. In both spatial and transform domain, different methods have been applied to modify a watermark according to the cover image. Early approaches of watermarking systems are not image adaptive and used global watermark strength for all selected coefficients of the image. Whereas these systems are known to be image adaptive. In this thesis we use GP and IT2FLS to calculate watermarking weight factor to balance imperceptibility and robustness.

2.1.3 Watermark domains

Watermarking schemes are usually based on spatial domain methods as well as transformed domain techniques such as Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) (Bracewell & Bracewell, 1986), and wavelet (Hsieh, Tseng, & Huang, 2001), (Kundur & Hatzinakos, 1998) etc. Watermarking in spatial domain is straight forward and easy to implement as compared to watermarking in transformed domain. Historically spatial domain watermarking was the first watermarking scheme the researcher had investigated upon. However, it has low robustness compared to transformation domain as the watermark easy be obliterated by lossy image compression techniques. Moreover, polynomial transformation based watermarking techniques are proposed by researchers to obtain improved imperceptibility and robustness. In this thesis our focus is on transform based watermarking techniques.

Stereo image based domain (also called 3D imaging) watermarking techniques are also very active research area. Stereoscopy denotes a system for generating or enhancing the

delusion of depth of an image by offering two offset images separately to the left eye and right eye of the observer. These 2D images are then unified in the brain to contribute the perception of 3D depth. The second type of 3D image representation is called DIBR 3D image. DIBR consist of a center image and a depth image. In the literature many stereo image based watermarking techniques have been proposed but very little work has been done in watermarking DIBR 3D image Representation. Usually a watermarking technique is intended in view of its applications with certain requirements.

2.1.4 Watermarking applications

As compared to other technologies watermarking has got a number of applications to its advantage. Watermarking application consists of copyright control, temper detection, owner identification, device control and transaction tracking. An application has to deal with a particular sequence of alterations, these alteration are generally categorized as watermark attack.

2.1.5 Attacks category and their countermeasure

Watermark data is vulnerable to attacks in different ways. An attack is any attempt that eradicate, erase the watermark and make its detections extremely difficult. (Barni & Bartolini, 2004) have dealt upon the types and levels of robustness in detail, which require a particular watermarking application. For a certain watermarking setup, there are some set of attacks along with their countermeasures. In the face of distortions certain strategies are used to make a watermark system consistent. For example redundant embedding of watermark, selection of perceptually significant coefficients for optimum imperceptibility and robustness, spread spectrum modulation and inverting distortion in detection phase for ease in watermark retrieval process.

(Voloshynovskiy, Herrigel, Baumgaertner, & Pun, 2000), (Kutter & Petitcolas, 1999) has classified attacks in to 4 categories as under. (a) Removal and interference attack, (b) geometrical attack, (c) cryptographic attack, (d) protocol attacks as shown in the Table 2.1 below.

As comparing to common signal processing attacks, intentional tempering is difficult to resist. However, watermark attacks and their counter measure are intricate and still a top of research. In order to evaluate the potential of a watermarking technique in face of robustness many hypothesis are made specifically about the attacker. For example if attacker has the knowledge of watermarking algorithm, he has detector that can modify and what tools he may have?

Table 2.1: Watermarking Attack Classifications

Classification of watermarking attacks		
Active Attack	(a) Removal Attack	<ul style="list-style-type: none"> • Denoising/filtering <ul style="list-style-type: none"> ○ ML based(maximum likelihood) <ul style="list-style-type: none"> ▪ Local mean(averaging) ▪ Median ▪ Trimmed mean ▪ Myriad filter ○ MAP based(a maximum a posteriori probability) <ul style="list-style-type: none"> ▪ Adaptive wiener filter ▪ Hard and soft shrinkage ▪ ○ MMSE based (a minimum mean square error) • Lossy compression • Quantization • Remodulation <ul style="list-style-type: none"> ○ Median filter(remove high frequency part) ○ Wiener filter • Collusion • Averaging <ul style="list-style-type: none"> ○ Statistical
	(b) Geometric Attack	<ul style="list-style-type: none"> • Global, local distortion <ul style="list-style-type: none"> ○ Rotation, scaling, change of aspect ratio, translation, shearing, line/column removal, cropping, random bending. • global ,local warping <ul style="list-style-type: none"> ○ circular shift

		<ul style="list-style-type: none"> • global, local transform • jittering
	(c) Cryptographic Attack	<ul style="list-style-type: none"> • brute force key search <ul style="list-style-type: none"> ◦ exhaustive search to find secret information • oracle <ul style="list-style-type: none"> ◦ creation of non-watermark image
Passive Attack	(d) Protocol Attacks	<ul style="list-style-type: none"> • watermark inversion <ul style="list-style-type: none"> ◦ extract watermark from non-watermarked image • copy attack <ul style="list-style-type: none"> ◦ copying the estimated watermark on target data

One has to effectively deal with watermark attack because an attack make it difficult to detect the watermark in the watermark detection phase. Watermark detection phase tries to reveal the hidden watermark in an image. The watermark detection phase may or may not require the original image for watermark detection.

2.1.6 Blind watermark detection

Blind watermark detection is a process in which a watermark is detected without the aid of reference image. It is a more practical approach as compared to non-blind watermark detection approach as in most of the scenarios the reference image may not be timely available. In our work blind watermark detection is used.

2.2 Properties of Human Visual System/ Perceptual modelling of a digital watermark

The human visual system comprises of mainly human eye and some part of human brain. The eye act as camera and brain perform the image processing operation. Figure 2.1 shows human eye cross section.

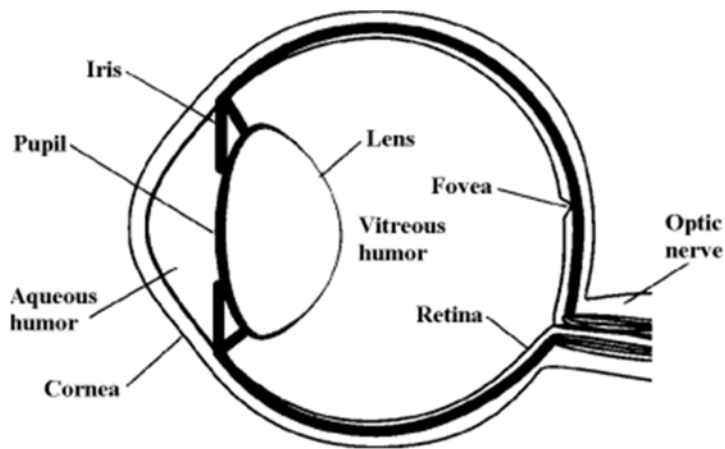


Figure 2.1: Human Eye and its different parts (Maintz, 2002)

Our eyes identify a scene when light rays are reflected from that scene. These rays should lie in range of visible spectrum that is 300 to 700 nanometer of electromagnetic spectrum. On receiving a ray in this range our eye sends a signal to brain through optic nerve.

After entering into the eye the ray then passes through different parts of eye before reaching retina, where photoreceptors convert the rays into electrical signals. There are two kinds of photoreceptors in human eye these are called rods and cones. Hundreds of millions of rods are spread across the retina while in fovea region millions of cones are located which can distinguish between different colors. This is possible due to three different types of cones which are sensitive to different wavelengths of electromagnetic spectrum. Because of these three different kinds of cones human eye can perceive and differentiate between different colors.

2.2.1 Luminance

Generally, Luminance is a measure which describes the amount of light that passes through and falls on a unit area. Light consists of a spectrum at different wavelengths. Human visual system usually responds to light at wavelengths which lie in specific range

that is between 400 nm to 700 nm. Visual sensitivity is function of wavelet. Luminance is usually measured in candela per square meter (cd/m²) which is standard unit for luminance measurement.

We used concept of luminance or brightness to invisibly embed the watermark. HVS is less sensitive to areas of image, with high or low brightness area (Belkacem, Dibi, Bouridane, & Ieee, 2007).

2.2.2 Contrast

Contrast (Peli, 1990) is a basic perceptual property of a digital image. There are different ways to calculate contrast. The Michelson formula to calculate contrast in simple pattern i-e periodic pattern can be given as:

$$C = \frac{L_{\max} - L_{\min}}{L_{\max} + L_{\min}} \quad 2.3$$

Where the L_{\max} and L_{\min} are the maximum and minimum luminance values in the periodic pattern. The weber fraction formula for local contrast calculation, of a single point, object or visual target having constant luminance and background is given as:

$$C = \frac{\Delta L}{L_{\min}} \quad 2.4$$

where, ΔL is the change in the object luminance.

Another term commonly used to describe Contrast is Contrast masking: The word masking is used for the interference or interaction of two stimulus that are passing through the same space and at the same interval of time. The effect of this interaction may be decrease or increase in the brightness, failure to detect of one stimulus due to masking effect of another stimulus (Legge & Foley, 1980). Low contrast masker increase the

detectability of a signal (Nachmias & Sansbury, 1974). For high contrast masker and signal at medium and high spatial frequencies, the signal threshold elevation to masker is maximum when masker and signal have the similar or equal level of frequency. Threshold elevation declines repeatedly as the masking frequency move away from the signal frequency.

2.2.3 Entropy

Entropy characterize the extent of information in a signal. The entropy was employed in quantification of information by Claude Shannon. Shannon (1948) introduced the probabilistic notion in modeling message communication. According to his assumption, information can be represented as a probabilistic process. If a receiver is designed for gathering all probable messages, it is important to know the probability of each message occurring. To isolate single message (m) from all possible messages in a set, the existence of this random event k is the probability $P(m)$ of the message. The self-information of k is the quantity $I(m)$. It means that the amount of self-information of m is inverse to the probability of m . If the event k always occurs, $P(m)=1$, no (new) information can be transferred. The logarithmic measurement is only accomplished for mathematical ease. In a discrete or continuous source of information, self-information for each m_i element in a set of messages can be formulated as (Leung, King, & Vohora, 2001):

$$I(m_i) = \log \frac{1}{P(m_i)} = -\log P(m_i), \quad 2.5$$

If there are large number, Z , of elements in a set of messages, by the Law of Large Numbers, the expected number of m_i will be $ZP(m_i)$ times. So, the average self-information in that set of messages with Z outputs can be represented as:

$$I(m) = -ZP(m_1)\log P(m_1) - ZP(m_2)\log P(m_2) - \dots - ZP(m_n)\log P(m_n), \quad 2.6$$

The summation of the self-information of all the elements is the value for that set, H, which is the average information per source output.

$$H = -Z \sum_{i=1}^n P(m_i) \log P(m_i), \quad 2.7$$

The value (H) escalates, with rise in the number of elements and thus more information is accompanying with the source. Further, if the probability of each element is similar, the entropy is maximized and the source provides the maximum possible average information per element. In fact, to certain extent, Shannon's entropy (equation 2.7) is the same as thermodynamic entropy (see equation 2.8).

$$S = -m \sum_i p_i \ln p_i \quad 2.8$$

$$m = 1.38 \times 10^{-23} \text{ J / K}$$

Although their principles and generalizations are different, Shannon's value H is still named entropy. But in the computation, there are some arrangements. Constant Z is the Boltzmann constant in thermodynamic entropy. However, to measure the information content, this constant is set to unity. And the logarithm's base is determined by the choice of unit for the information. For the digital manipulation a base of 2 is appropriate, and yields the unit of bit. Furthermore, to linearize the result, the natural logarithm of probability is used. Finally, Shannon's entropy is defined as (Leung et al., 2001).

$$H = - \sum_{i=1}^n P(m_i) \ln_2 P(m_i), \quad 2.9$$

We used Matlab entropy function in our technique as given in the following equation:

$$E = -\sum_{i=1}^g p_i \cdot \log_2 p_i \quad 2.10$$

Where p is the (histogram) number of occurrences of particular normalized frequency component contain in an image. Where i range from 1 to the number of frequency level g .

We used the concept of entropy to embed the watermark imperceptibly. Higher the value of entropy means large concentration of information in that part of image. HVS is less sensitive to modification to that part of image. So embedding watermark in the areas of image having higher value of entropy will be less visible (Akhbari, Ghaemmaghan-Ii, & Ieee, 2006).

2.2.4 NVF

Noise Visibility Function is the function that describes local image properties, categorizing texture and edge regions where the watermark should be more intensely embedded (Voloshynovskiy et al., 2000). Since watermarking process have strong relationship with the local image properties thus NVF based on not pure stationary Gaussian model, more suits for watermarking problem. Supposing the cover image is a Gaussian process. The NVF can be inscribed as:

$$NVF(i, j) = \frac{w(i, j)\sigma_n^2}{w(i, j)\sigma_n^2 + \sigma_x^2(i, j)} \quad 2.11$$

Where σ_n^2 is the noise variance, $\sigma_x^2(i, j)$ is the local variance of the image in a window centered on the pixel with coordinates (i, j) , and $1 < (i, j) < N$. whereas $w(i, j)$ is weight function depends on shape parameter $\gamma \cdot w(i, j)$ can be described as:

$$w(i, j) = \gamma [\eta(\gamma)]^\gamma \times \frac{1}{\|r(i, j)\|^{2-\gamma}} \quad 2.12$$

where

$$r(i, j) = \frac{x(i, j) - \bar{x}(i, j)}{\sigma_x}$$

$$\eta(\gamma) = \sqrt{\frac{\Gamma\left(\frac{3}{\gamma}\right)}{\Gamma\left(\frac{1}{\gamma}\right)}}$$

where

$$\Gamma(t) = \int_0^{\infty} e^{-u} u^{t-1} du$$

$\Gamma(t)$ is gamma function. The factor γ is called the shape parameter, and $\bar{x}(i, j)$ is the local mean of the image. Whereas the non-stationary Gaussian Model can be represented as

$$NVF(i, j) = \frac{1}{1 + \sigma_x^2(i, j)} \quad 2.13$$

Where σ_x^2 is the local variance of the image in a window centered on the pixel with coordinates (i, j) . Since watermarking process have strong relationship with the local image properties thus NVF based on non-stationary Gaussian model better realized for watermarking problem. The computed value of NVF, represent allowable distortion for each pixel of the image.

Usually high local variance value indicate presence of texture and edge region. So in flat regions, the NVF tends to 1, and for edge and textured areas it tends to 0, since we anticipate that the watermark alterations are more perceptible in flat regions and less

noticeable in texture regions. According to (Voloshynovskiy et al., 2000) the watermark inserted in texture or edge regions is stronger than in the flat regions. If embedding maximum permissible watermark in each pixel, the robustness of watermarking will be high. The most widely NVF formula use in image application are

$$NVF(i, j) = \frac{1}{1 + \theta \sigma_x^2(i, j)}, \quad 2.14$$

Where θ is the tuning parameter, which act as contrast adjustment parameter in NVF.

Its value can calculated as

$$\theta = \frac{D}{\sigma_{x \max}^2} \quad 2.15$$

where $\sigma_{x \max}^2$ is the maximum local variance and value of D lies in the range of 50 to 100 inclusive.

2.2.5 Watson perceptual model

Perceptual model for the discrete wavelet transform divides an image into different subbands based upon transformation level and orientation. The transformation level λ and orientation level θ is related to the corresponding subband such as LL, HL, HH and LH subbands. According to perceptual model (Liu, Karam, & Watson, 2006) the contrast masking effect for every (i, j) DWT coefficient can be computed as follows:

$$a_c(\lambda, \theta, i, j) = a_{c_self}(\lambda, \theta, i, j) \cdot a_{c_neig}(\lambda, \theta, i, j) \quad 2.16$$

Where $a_{c_self}(\lambda, \theta, i, j)$ denotes self-contras masking factor and $a_{c_neig}(\lambda, \theta, i, j)$ Neighborhood masking factor.

$$a_{c_self}(\lambda, \theta, i, j) = \max\left\{1, \left(\frac{|\mathcal{G}(\lambda, \theta, i, j)|}{JND_{\lambda\theta} al(\lambda, \theta, i, j)}\right)^\varepsilon\right\} \quad 2.17$$

$$a_{c_neig}(\lambda, \theta, i, j) = \max\{1, \sum_{\kappa \in \text{neighbourhood}(\lambda, \theta, i, j)} \frac{\left(\left| \frac{\mathcal{G}(\kappa)}{JND_{\lambda\theta} a_l(\lambda, \theta, i, j)} \right| \right)}{N_{i,j}}\} \quad 2.18$$

Coefficients in the same sub-bands that lie within a window centred at the location (i, j) , $N_{i,j}$ denotes the number of coefficients in that neighbourhood, $\mathcal{G}(\lambda, \theta, i, j)$ is the DWT coefficient value at location (λ, θ, i, j) , and ϵ is a constant that controls the influence of the amplitude of each neighbouring coefficient. For the LL sub-band, contrast masking is suppressed by setting $\epsilon = 0$. For other sub-bands, it is set to 0.6. Equation 2.16 performs the contrast masking. Just noticeable distortion (JND) threshold is formulated as specified in (Liu et al., 2006).

$$JND_{\lambda, \theta}(r) = \frac{1}{A_{\lambda, \theta}} a \cdot 10^k \left\{ \log_{10} \left(g_{\theta} f_0 2^{\lambda/r} \right) \right\}^2 \quad 2.19$$

Where a, g_{θ}, k, f_0 are constants, for the amplitude of the DWT 9/7 basis function relevant to level λ and orientation θ , and r is the visual resolution of the display in pixels/degree it can be represented as

$$r = d\nu \tan\left(\frac{\pi}{180}\right) \approx d \frac{\nu\pi}{180} \approx d \frac{\nu}{57.3} \quad 2.20$$

Where ν represent the viewing distance in cm and d represent the display resolution in pixels/cm.

Table 2.2 list the $A_{\lambda\theta}$ values for a six level DWT decomposition. Table 2.3 list the constants.

Table 2.2: Basic function $A_{\lambda\theta}$ amplitude for 6-level 1st level for a 9/7 dwt (Liu et al., 2006).

Orient	DWT Decomposition Level					
	1	2	3	4	5	6
LL	0.621	0.345	0.180	0.091	0.0459	0.0230
LH,HL	0.672	0.413	0.227	0.117	0.0597	0.0300
HH	0.727	0.494	0.286	0.152	0.0777	0.0391

Table 2.3: Parameters for DWT threshold model (Liu et al., 2006).

a	k	f	g _{LL}	g _{HL,LH}	g _{HH}
0.495	0.466	0.401	1.501	1.0	0.534

Luminance masking is performed using the equation 2.21, it estimate and kept the appropriate level to which luminance masking will take place and α takes value of 0.649 as suggested in (Liu et al., 2006). Whereas $\hat{g}_{\lambda \max, LL_{i,j}}$ represent the coefficient value in LL sub-band is that spatially corresponds to the location (λ, θ, i, j) . For each DWT transformed coefficient, at location (i, j) within subband (λ, θ) where, λ is the transform level and θ is the orientation perform the luminance masking using equation 2.21,

$$a_i(\lambda, \theta, i, j) = \left(\frac{\hat{g}_{\lambda \max, LL_{i,j}}}{\hat{g}_{mean}} \right)^{\alpha T} \quad 2.21$$

where

$$\hat{g}_{\lambda \max, LL_{i,j}} = g_{\lambda \max, LL_{i,j}} / Q_{\lambda \max, LL}$$

and

$$\hat{\mathcal{G}}_{mean} = \mathcal{G}_{mean} / Q_{\lambda \max} LL$$

$$Q_{\lambda \theta} = JND_{\lambda \theta}$$

2.3 Perceptual Modelling using Artificial Intelligence techniques (AI)

The following section describe GP, Perceptual model and Fuzzy in detail.

2.3.1 Genetic Programming

Genetic programming (GP) (Koza, 1992), (Banzhaf, Nordin, Keller, & Francone, 1998) inherits properties from evolutionary computing techniques (genetic algorithms) and automatic programming. GP is an organized routine, work automatically to accomplish solution of a problem beginning from a high-level statement of what necessities to be done. To solve a problem GP genetically spawns a set of computer programs. These set of computer programs are called population. GP iteratively transmutes a population of computer programs into a new generation of programs by using referents of naturally occurring genetic operations. The standard genetic operations comprise of crossover, reproduction, mutation, gene deletion, gene duplication.

The structure of programs in GP are syntax trees. The syntax tree consist of Nodes and links. The nodes specify the Instructions to execute. The links specify the parameters or arguments for each instruction. The last node of a tree are termed as tree's leaves or terminals. In a more complex forms of GP, programs can be collected as a set of trees, clustered together under a distinctive node termed root of the tree.

2.3.2 Typical representation of a genetic program

This subsection describe some of the common terms used to describe Genetic program.

- **Terminals and function**

In GP, program is created from terminal set and function set. Generally the terminals are independent variables of the problem, constants or external inputs. While the function set may consist of problem related functions or simply the arithmetic functions of addition (+), subtraction (-), multiplication (\times), and division (\div) as well as a conditional branching operator.

- **Program generation**

For the program generation, user needs to specify the control or input parameters for the program execution. The most significant input parameter is the population size. Additional input parameters comprise the probabilities of performing the genetic operations, the maximum size for programs, that is the maximum depth level of the tree and other details of required for the GP execution. Programs can be generated using different methods e.g. Full method, Grow method, Ramped half and half method.

- **Genetic operators**

Preliminary population which is generated has very little fitness value so different genetic operators are used to breed programs. It include reproduction, cross over and mutation operators. In reproduction process a program in one generation is carefully chosen and moved to next generation as it is i-e it is copied to succeeding generation. While in crossover process, the best features are selected from different programs in a population and create a new program out of it and move this new program into next generation i-e exchange of subtree between two trees as a result these two trees are new

two different programs and can be transferred to next generation. In mutation replacement of a function or terminal takes place.

- **Fitness**

Fitness is the extent how well a program produce output from the particular set of input. Fitness measure implicitly identifies the search's preferred goal. Fitness of a program is calculated using fitness function. Fitness function depend upon the problem. For a given set of problems the Fitness function varies.

- **Termination criterion**

The termination condition may comprise a maximum number of generations to be run as well as achieving a problem related state. The individual which is termed as best so far are put together and termed as the output result of the run.

Genetic programming iteratively transmutes a population of computer programs into a new generation of the population by applying correspondents naturally occurring genetic operations. These operations are applied to individuals carefully chosen from the population. The individuals are probabilistically selected to participate in the genetic operations based on their fitness. The iterative transformation of the population is executed inside the main generational loop of the run of genetic programming. GP simulation and search flow process are shown in Figures 2.2 and 2.3.

2.3.3 A basic GP algorithm

- 1. Create and initialize the population of individual computer programs.*
- 2. Appraise each single program in the existing population. Allocate fitness to each program.*
- 3. till new population is entirely generated, repeat the following*

- *Select program in the existing generation*
 - *Apply genetic operators on the particular selected programs.*
 - *Insert the result of the genetic operations into new generation.*
4. *If termination condition is not satisfied, reiteration of step 2 to 4 with new generation.*
5. *The best single program in population is the output.*

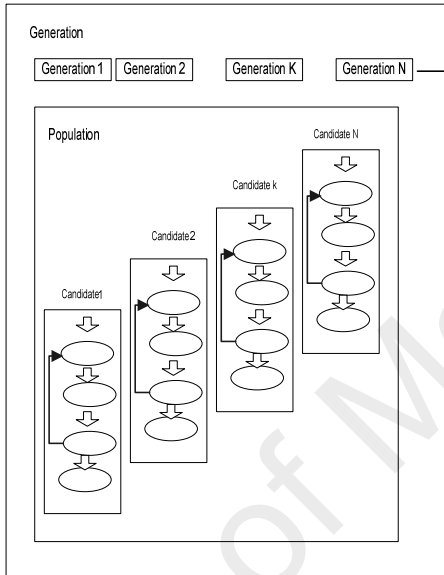


Figure 2.2: GP Simulation for evolving best candidate.

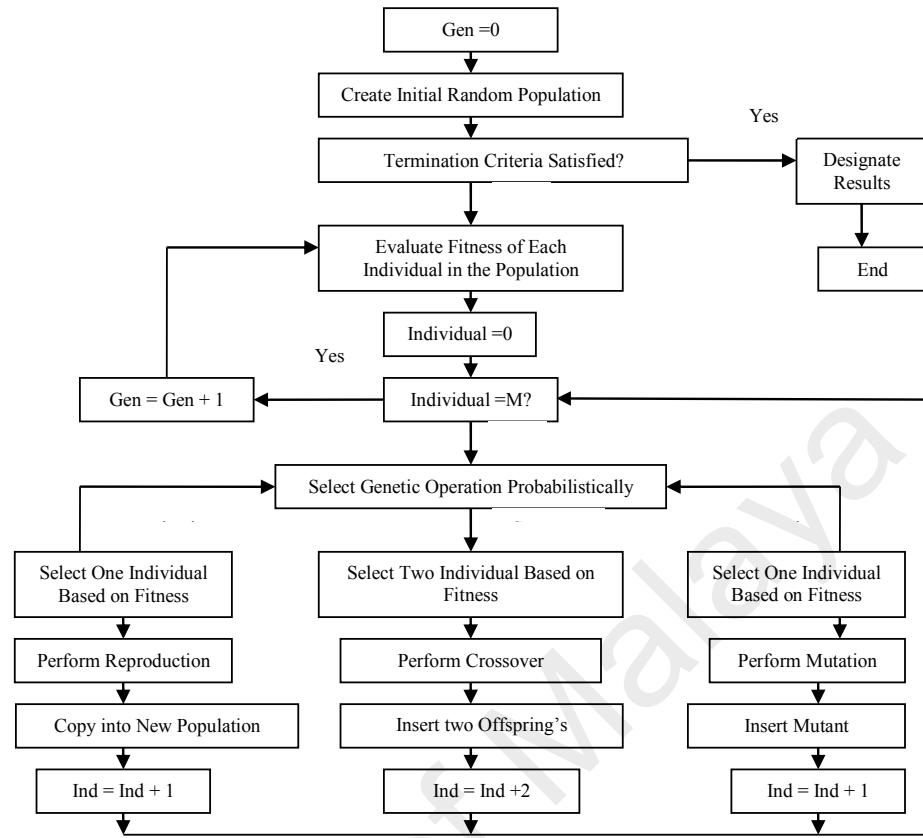


Figure 2.3: GP search flow (Khan, Mirza, & Majid, 2006).

2.3.4 Perceptual model based watermarking techniques

Watermarking algorithms (Podilchuk & Delp, 2001) are usually designed in two domains. Spatial domain (Nikolaidis & Pitas, 1998), (Barni, Bartolini, & Piva, 2001), (Darmstaedter, Delaigle, Nicholson, & Macq, 1998), (Wolfgang & Delp, 1996) and transform domain, also called frequency domain (Piva, Barni, Bartolini, & Cappellini, 1997), (Kundur & Hatzinakos, 1998), (Hernandez, Amado, & Perez-Gonzalez, 2000). In spatial domain, the information is added directly in the pixel value while in transform domain, the information is embedded in the coefficient after transforming the pixels such as DCT, DFT or Discrete Wavelet Transformation (DWT) etc. The watermark is usually embedded in middle frequency part of the image. As changes made to low frequency part i-e., LL sub-band can easily be visible to human eye, while the high frequency part i-e., HH sub-band is more sensitive to compression and scaling operation. The main

requirement of any watermarking system is imperceptibility and robustness. But these requirements cannot be obtained at same time as both properties are complement to each other and offer a trade-off. When we increase one, the other decrease and vice versa. Therefore a compromise between these characteristics needs to be found to achieve the optimal level of watermark strength. A number of different block based watermarking techniques have been proposed in literature (Ghazy, El-Fishawy, Hadhoud, Dessouky, & Abd El-Samie, 2008), (Podilchuk & Zeng, 1998).

(Piva et al., 1997) Proposed a technique in which embedding is performed in the DCT domain. Zigzag scan DCT coefficients are obtained in a vector form and the first $(l+m)$ coefficients are selected, where l and m represent any number, while $l+m$ represent a range of coefficients selected for the watermark embedding. To make a tradeoff between the robustness and imperceptibility, the last m coefficients are selected for embedding. Detection of watermark has performed using correlation.

(Usman & Khan, 2010) Introduced a technique in which visual tuning of a watermark is made in DCT domain. GP is used for watermark structuring on the basis of cascading attack and HVS characteristics. Bose, Chaudhuri, and Hocquenghem (BCH) codes are used to encode the message. (Woo, Du, & Pham, 2005) Proposed a simplified embedding technique, which significantly decreases the embedding time while maintaining the performance of imperceptibility and robustness. This technique take into account implicit features of DWT sub-bands to mimic HVS characteristics. (Huang, Pan, & Chu, 2007) Proposed a technique while considered imperceptibility, robustness and capacity for watermark embedding. Genetic Algorithm (GA) is used to select appropriate coefficient position using tradeoff between these three factors. Then, binary watermark is embedded in DCT domain. The drawback of this scheme is that they do not consider the appropriate level of watermark strength for each coefficient.

Singular Value Decomposition (SVD) based optimized watermarking technique is proposed in (Aslantas, 2008) for gray scale images to get optimal balance between robustness and imperceptibility. GA is used to obtain optimal multiple scaling factors to get best level of robustness and imperceptibility. They used Correlation method as fitness function. In (L. Li, Xu, Chang, & Ma, 2011), a redistributed invariant wavelet domain is proposed by authors to resist geometric attacks, which can change the value of pixels such as rotation, flipping etc. They applied existing wavelet based techniques on redistributed invariant domain and show that the new domain is more resistant to geometric attacks.

In (Keyvanpour & Merrikh-Bayat, 2011) the author proposed block based watermarking technique, in this technique they selected those pixels which are related to edges in discrete wavelet transformation domain for watermark embedding. Robustness is achieved by embedding multiple copies of watermark. Embedding in the edge region is less visible to human eye so imperceptibility criterion is achieved as well.

To obtain robustness, the authors in (W.-H. Lin, Wang, Horng, Kao, & Pan, 2009) suggested to randomly choosing blocks while keeping the local maxima relationship in a block by embedding watermark of different energy in different wavelet (Peng, Li, & Yang, 2012)et coefficients. To keep the secrecy of the embedding location of watermark, blocks of different sizes are used.

To increase the embedded watermark capacity, authors in (Peng et al., 2012) proposed a reversible data hiding technique, which can tune selected integer transform parameters such that it can adaptively embed the watermark, using the block type information. The block types are categorized according to some pre-estimated distortion.

In (Shen & Chen, 2012) the authors try to consider all three important parameters of watermarking, i.e., robustness, capacity and imperceptibility. An improved pixel-wise

masking model, based on dual watermarking technique is developed. They obtain robustness by embedding watermark in selected wavelet coefficients and due to the dual watermarking, the capacity of watermark increases.

To preserve affine transformation and to resist affine transformation attack, the yang et al. (Yang, Song, Fang, & Yang, 2010) proposed a code division multiplexing algorithm (CDMA) based technique using barycentric coordinate representation for the image in a discrete biorthogonal wavelet domain.

The authors (Urvoy, Goudia, & Atrousseau, 2014) proposed DFT based blind and robust watermarking technique to improve the tradeoff between invisibility versus robustness of a watermark system. They use different characteristics of HVS such as contrast sensitivity and Psychometric function to optimally adjust the subjective visibility level of embedded watermark.

2.3.5 Fuzzy logic

Fuzzy logic is a fundamental tool to model nonlinear systems. Zadeh introduce the logic of type2 fuzzy system. It is an extension of type1 fuzzy system. IT2FLS is powerful tool to handle uncertainties that comes from different sources such as measurement uncertainty, process uncertainty, estimate uncertainty and implementation uncertainty (Castro, Castillo, & Melin, 2007).

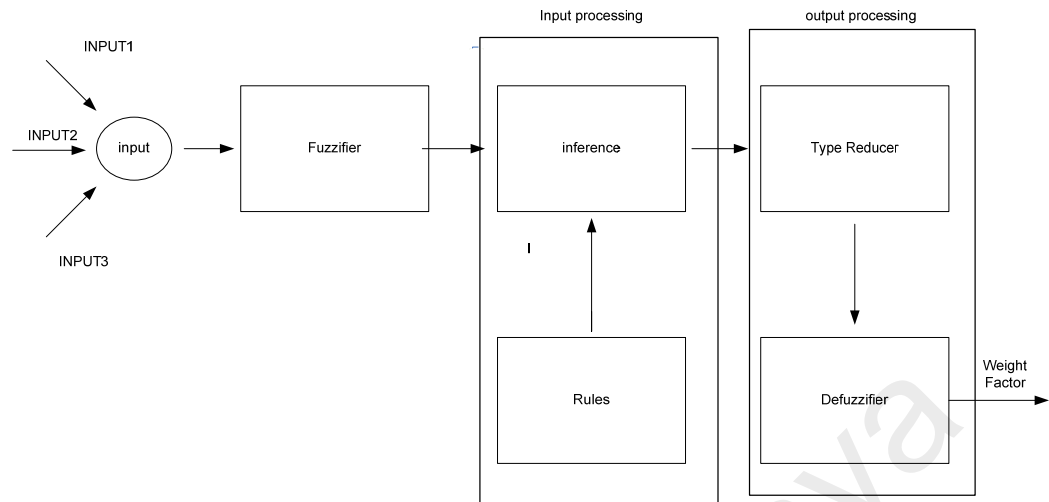


Figure 2.4: Overview of IT2FLS.

A type-2 membership function consist of, a primary and secondary type1 membership function. The job of the secondary membership function is to define all the possibilities for the higher order membership function. Which increase the type2 fuzzy system capability to handle uncertainties in data/information in a more logical /useful manner. Increased fuzziness in a description means increased ability to handle imprecise information in a rationally precise manner. We can apply three basic operations on the fuzzy set, which result into the creation of another fuzzy set. It includes union or join, intersection or meet and negation operation/operators.

A type-2 FLS comprises fuzzifier, rule base, fuzzy inference engine, and output processor as shown in Figure 2.4. In fuzzifier the membership function convert the crisp values of input parameters to fuzzy values. The IT2FL includes 22 built-in Interval Type-2 Membership Function (IT2MF) types. These 22 functions are, in turn, constructed from numerous basic functions such as the sigmoid curve, piecewise linear functions, the Gaussian distribution function, cubic polynomial curve , and quadratic and. A type-2 FLS can described or explained by IF–THEN rules, but rules antecedent or consequent sets

are type-2. Type-2 FLSSs can be used when the situations are too undefined to define precise membership grades such as when training data is degraded by noise.

The output processor includes type-reducer and defuzzifier, it creates a type-1 fuzzy set output (from the type-reducer) or a number (from the defuzzifier). Interval Type-2 Fuzzy inference is the routine to formulate the mapping from a given input to an output using interval type-2 fuzzy logic. The mapping then provides a basis from which decisions can be made, or patterns discerned. There are two types of fuzzy inference systems that can be realized in the Interval Type-2 Fuzzy Logic Toolbox: Mamdani-type and Sugeno-type. These two kinds of inference systems differ slightly in the way outputs are determined. Interval Type-2 Fuzzy inference systems have its application in diverse areas such as automatic control, data classification, decision analysis, expert systems, and computer vision (Mendel, 2001).

2.4 RST Invariant Domain

This section discuss in detail robust image watermarking techniques and RST invariant domain such as RT and polynomial transform domain.

2.4.1 Robust image watermarking and RST attacks

Robust watermarking has application in copyright protection. To protect copyright the watermark should persist and resist common image processing variations, including intentional and unintentional attacks.

The various kind of operations performed on the watermark image are termed attack. An attack may degrade the watermark image. This degradation can be induced using noise addition, cropping, row and column removal. Other kind of attack may enhance the image to desynchronize the watermark. Image enhancement operations include sharpening, smoothening, median filtering and contrast enhancement. Image compression

is also a kind of attack in which watermark information may be lost and could not be recovered specially in lossless compression. JPEG is one of the common compression attack on digital images. Geometric transformation such as rotation, scaling and translation also regarded as RST attack. Robustness against RST is an immense challenge for the watermark community (Zheng, Liu, Zhao, & Saddik, 2007), (C.-Y. Lin et al., 2001), (H. S. Kim & Lee, 2003). Other transformations such as aspect ratio change, shearing, reflection, projection and random bending also poses serious distortion to watermark.

Lop polar mapping (LPM) has been using in watermarking application due to its rotation invariance characteristics. LPM transform rotation operation into linear shift operation. And any domain which is shift invariant can become rotation and shift invariant. We have use LPM with the RT in chapter 4 to improve RT resistant to rotation attacks.

2.4.2 Watermarking techniques using RST invariant domain

The watermarking techniques are useful for purposes of content authentication and copyright protection. The embedded watermark should be robust against a variety of attacks, including geometrical attack, noise addition attack, JPEG compression attack, filtering, cropping and statistical attacks. Therefore, robust watermarking has been a major research direction for many years. However, robustness against geometrical attack, particularly RST, remains as a technically challenging task due to the simplicity of RST operations and their damaging effect on the embedded watermark information. In addition, blind watermark detection is the preferred and more practical approach when compared with non-blind watermark detection because the former does not require the original unprocessed image.

RST invariant technique has been proposed by different researchers. Some of them tried to solve this problem by proposing new transform domain such as Fourier mellin transform domain and Log polar Mapping (LPM) of the Fourier transform domain (Ruanaidh & Pun, 1998), (C.-Y. Lin et al., 2001; Zheng et al., 2007)).

Robust watermarking methods can be broadly categorized into two classes, namely, feature-based methods, and invariant domain methods. Feature-based methods rely on a resynchronization step during watermark detection (Zheng et al., 2007), (Pham, Miyaki, Yamasaki, & Aizawa, 2007), (L. Li et al., 2011), (Haijun, Xingming, Hengfu, & Zhihua, 2011). This step increases the computational load and processing time of the watermarking methods. On the other hand, invariant domain methods depend on the invariant properties of the transformation considered during the watermark embedding and detection processes (Woo, Du, & Pham, 2006), (Bas, Chassery, & Macq, 2002). Therefore, invariant domain methods are independent from the image contents and its features. This property is advantageous especially for watermarking images without distinctive features. A few work (Woo et al., 2006), (H. S. Kim & Lee, 2003), (Nelson & Kingsbury, 2011) focusing on global invariant characteristic exist in the literature.

Robust watermarking methods using the RST invariant domain are relatively rare compared with the feature-based methods because it is technically challenging to devise a RST invariant domain. Among the robust watermarking methods which were devised in the RST invariant domain, some techniques utilize the local invariant characteristics to produce robust watermarking but they are fundamentally feature based techniques. For feature based RST invariant techniques, a few notable methods are examined here. (Yuan & Pun, 2012) proposed a feature extraction-based method for geometric invariant watermarking. Robust feature points in small circular areas are extracted using Harris corner detector. Zernike transformation is then applied to the selected normalized binary

form of the detected features to minimize the reconstruction error of the Zernike transformation. However, only the three most robust feature points are evaluated for watermark detection to show its robustness against geometric attacks. Nonetheless, this method is basically feature-based, with geometric invariant characteristic for the selected local features. (Shi et al., 2012) presented a RST invariant watermarking technique using Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD). SVD is applied to the approximate subband of DWT at the l -th level of the host image. Then, an encrypted watermark is embedded in the diagonal matrix S of the SVD. To achieve robustness, SVD is again applied on the watermarked S matrix to produce the final watermarked image. However, this method requires the original cover image for watermark detection, i.e., non-blind. Another RST invariant watermarking technique was proposed by (Zhao, Ni, & Zhu, 2012), which utilizes the centroid moment and sector-shape partition. First, an image is divided into bitplanes. Then, the centroid moment of the most significant bitplane is calculated to achieve robustness against most of the image processing operations. In particular, the input image is divided into n number of segments based on the centroid value, where n is the total number of watermark bits. Finally, the watermark is embedded using Quantization Index Modulation (QIM). The resynchronization step in this method relies on two factors, namely, the centroid moment and the sectoring value. The centroid should be nearly constant and the reconstructed sectoring value should match to extract the watermark. Then (Yu, Ling, Zou, Lu, & Wang, 2012) developed a feature based rotation and scale invariant region for watermark embedding. They use Disk Rotation Scaling Invariant Features (DRSIF) features to construct invariant region for watermark embedding. To detect the embedded watermark, the DRSIF regions are constructed. If these regions are slightly altered, then it is impossible to detect the watermark accurately, or the watermark may not be detected at all.

Most of the methods reviewed above are not truly based on invariant domain because they are, in some manner, depend on the resynchronization step for detecting the embedded watermark. As such, frequency and spatial information provided by the wavelet subbands as well as the multi-scale analysis of wavelet transform motivated the construction of invariant domain in the wavelet domain. Other transformations such as DFT only offer frequency information and the lack spatial information. Moreover, they are also incapable in providing multi-scale analysis. Despite very few wavelet transformations possessing the shift-invariant property, RT is found to be suitable for the purposes of invariant domain watermarking. Nonetheless, Fuzzy based watermarking techniques are proposed by many researchers to solve different issues related to the watermarking (Motwani & Harris Jr, 2009), (Oueslati, Cherif, & Solaiman).

To achieve a delicate balance between watermark robustness and imperceptibility requirement, we have designed an IT2FLS based model to calculate the watermark weights. We used different features such as NVF, perceptual luminance and entropy etc , of the selected coefficients to imperceptibly embed the watermark.

2.4.3 Riesz Transformation

The RT is translation, scale and rotation invariant. The translation invariance follows directly from the definition, while the scale invariance is verified in the Fourier Domain (Unser & Van De Ville, 2010). In addition, RT has the perfect reconstruction property. Let $f(x)$ be the d dimensional input signal in the continuous domain space of variable x , where $x = (x_1, x_2, x_3, \dots, x_d) \in \mathbb{R}^d$.

The multidimensional Fourier transformation of the input signal $f(x) \in L_1(\mathbb{R}^d)$ is defined as follows:

$$\hat{f}(\omega) = \int_{\mathfrak{R}^d} f(x) e^{-f\langle \omega, x \rangle} d_{x_1} \dots d_{x_d} \quad 2.22$$

where $\omega = (\omega_1, \omega_2, \dots, \omega_d) \in \mathfrak{R}^d$. In our case, $d = 2$ is considered. The RT is the natural multidimensional extension of the Hilbert transform. The RT of a function $f(x) \in L_1(\mathfrak{R}^d)$ is the scalar to vector signal transformation $\hat{\mathfrak{R}}f(\omega)$. Its frequency domain definition is $\hat{\mathfrak{R}}f(\omega) = -j \frac{\omega_i}{\|\omega\|} \hat{f}(\omega)$, with $-j = \sqrt{-1}$. For the detail description please refer to (Chenouard & Unser, 2011).

RT has the properties of invariance i-e it is translation and scale invariant. Moreover RT rotation property has also been formalized (Unser & Van De Ville, 2010).

2.4.4 Watermarking techniques in polynomial transform domain

Polynomial is an expression or function made up of constant, variables and exponents. Which are called terms. These terms are connected together using different operations such as addition, subtraction, multiplication and non-negative exponent. Polynomial has vast applications in mathematics and sciences.

Researchers have also used polynomial based transformation for watermarking. The author in (Le, Krishnan, & Ghoraani, 2006) proposed chirp watermark detection using discrete polynomial phase transform (DPT). The DPT models the signal as polynomial. Watermark is represented by the phase of DPT. They found DPT detect watermark with high accuracy. The author proposed an image adaptive invisible watermark based on orthogonal polynomial transformation (OPT) in (Krishnamoorthi, April 2009). They generate Just Noticeable Distortion mask (JND) by taking into account the image features such as textures, edges, and luminance of the cover image in the OPT domain to embed the watermark imperceptibly.

- **Introduction to Fractional Calculus**

Fractional calculus is a mathematical discipline which deals with derivatives and integrals of arbitrary real or complex orders. The history of fractional calculus is 300 years old and genuine expansion and progression has seen in 19 century. During the last decade fractional calculus has been applied to different fields most noticeable among them are physics, biology, science, engineering, image processing and other fields (Hu Sheng October 26, 2011). One of the advantages of fractional calculus is that it can be well thought-out as a super set of integer order calculus. Thus fractional calculus has the potential to realize what the integer order calculus cannot.

As the fractional calculus is a term for the theory of integrals and derivatives of arbitrary order, which merge and generalize the notions of integer order differentiation and n-fold integration (Podlubny, 1999).

The infinite sequence of n-fold integrals and n-fold derivatives are:

$$\dots \int_a^t d\tau_2 \int_a^{\tau_2} f(\tau_1) d\tau_1, \int_a^t f(\tau_1) d\tau_1, f(t), \frac{df(t)}{dt}, \frac{d^2 f(t)}{dt^2}, \dots \quad 2.23$$

The derivative of arbitrary real order α can be considered as an interpolation of this sequence of operators; the notation used for it namely

$${}_a D_t^\alpha f(t). \quad 2.24$$

The short name for derivatives of arbitrary order is fractional derivatives.

The subscripts α and t designate the two limits related to the operation of fractional differentiation; these are called terminals of fractional differentiation.

The fractional integral of order $\beta > 0$ can be denoted as

$${}_a D_t^{-\beta} f(t)$$

2.25

- **Properties of Fractional Derivatives**

The properties of fractional order integration and differentiation which are most often used are as follows (Podlubny, 1999).

(a) **Linearity:**

Like integer order differentiation, fractional differentiation has linear operation:

$$D^P (\lambda f(t) + \mu g(t)) = \lambda D^P f(t) + \mu D^P g(t), \quad 2.26$$

Where D^P represents any mutation of the fractional differentiation considered. The linearity of fractional differentiation follows directly from the corresponding definition. For example for the Grunwald- Letnikov fractional derivatives we have

$${}_a D^P (\lambda f(t) + \mu g(t)) = \lim_{\substack{h \rightarrow 0 \\ nh = t-a}} h^{-P} \sum_{r=0}^n (-1)^r \binom{P}{r} (\lambda f(t-rh) + \mu g(t-rh)) \quad 2.27$$

$$= \lambda \lim_{\substack{h \rightarrow 0 \\ nh = t-a}} h^{-P} \sum_{r=0}^n (-1)^r \binom{P}{r} f(t-rh) + \mu \lim_{\substack{h \rightarrow 0 \\ nh = t-a}} h^{-P} \sum_{r=0}^n (-1)^r \binom{P}{r} g(t-rh) \quad 2.28$$

$$= \lambda {}_a D_t^P f(t) + \mu {}_a D_t^P g(t). \quad 2.29$$

Similarly for Riemann Liouville fractional derivatives of order α we have

(b) **The Leibniz rule for fractional derivatives**

Let us take two functions and start with the known Leibniz rule for evaluating the n -th derivative of the product:

$$\frac{d^n}{dt^n}(\varphi(t)f(t)) = \sum_{k=0}^n \binom{n}{k} \varphi^{(k)}(t) f^{(n-k)}(t), \quad 2.30$$

where

$$\begin{aligned} \binom{n}{p} &= \binom{n-1}{k} + \binom{n-1}{k-1} \\ &= \frac{n!}{k!(n-k)!}. \end{aligned}$$

One of the useful consequences of the Leibniz rule for the fractional derivative of a product is a rule for evaluating the fractional derivatives of a composite function.

Let us take an analytic function $\varphi(t)$ and $f(t) = H(t-a)$, where $H(t)$ is the Heaviside function. Using Leibniz rule we can write:

$${}_a D_t^p \varphi(t) = \sum_{k=0}^{\infty} \binom{p}{k} \varphi^{(k)}(t) {}_a D_t^{p-k} H(t-a) \quad 2.31$$

$$= \frac{(t-a)^{-p}}{\Gamma(1-p)} \varphi(t) + \sum_{k=1}^{\infty} \binom{p}{k} \frac{(t-a)^{k-p}}{\Gamma(k-p+1)} \varphi^{(k)}(t). \quad 2.32$$

• Fractional Calculus Special Functions

Following are some of the most common special functions used in fractional calculus.

a) *Gamma Function*

One of the basic functions of the fractional calculus is Eulers gamma function $\Gamma(z)$, which generalize the factorial $n!$ and allows n to take also non-integer and even complex values.

The gamma function $\Gamma(z)$, can be defined by the integral

$$\Gamma(z) = \int_0^{\infty} e^{-t} t^{z-1} dt,$$

Which converge in the right half of the complex plane $\text{Re}(z) > 0$. Indeed, we have

$$\Gamma(x + iy) = \int_0^{\infty} e^{-t} t^{x-1+iy} dt = \int_0^{\infty} e^{-t} t^{x-1} e^{iy \log(t)} dt, \quad 2.33$$

$$= \int_0^{\infty} e^{-t} t^{x-1} [\cos(y \log(t)) + i \sin(y \log(t))] dt. \quad 2.34$$

The expression in the square brackets in above equation is bounded for all convergence at infinity is provided by e^{-t} , and for the convergence at $t=0$ we must have $x = \text{Re}(z) > 1$.

One of the basic properties of the gamma function is that it satisfies the following functional equation:

$$\Gamma(z + 1) = z\Gamma(z),$$

Which can be easily proved by integrating by parts:

$$\Gamma(z + 1) = \int_0^{\infty} e^{-t} t^z dt = \left[-e^{-t} t^z \right]_{t=0}^{t=\infty} + z \int_0^{\infty} e^{-t} t^{z-1} dt = z\Gamma(z). \quad 2.35$$

Obviously, $\Gamma(1) = 1$, and using equation 2.37 we obtain for $z=1, 2, 3 \dots$

$$\begin{aligned}
\Gamma(2) &= 1.\Gamma(1) = 1 = 1! \\
\Gamma(3) &= 2.\Gamma(2) = 2.1! = 2!, \\
\Gamma(4) &= 3.\Gamma(3) = 3.2! = 3!, \\
&\dots\dots\dots \\
\Gamma(n+1) &= n.\Gamma(n) = n..(n-1)! = n!
\end{aligned}
\tag{2.36}$$

Another important property of the gamma function is that it has simple poles at the points $z = -n, (n = 0, 1, 2, \dots)$. we can demonstrate this in the form:

$$\Gamma(z) = \int_0^1 e^{-t} t^{z-1} dt + \int_1^\infty e^{-t} t^{z-1} dt. \tag{2.37}$$

The first integral can be evaluated by using the series expansion for the exponential function. If $\text{Re}(z) = x > 0$ (i.e. z is in the right half-plane), then $\text{Re}(z+k) = x+n > 0$ and $t^{z+k} \big|_{t=0}$. Therefore,

$$\int_0^1 e^{-t} t^{z-1} dt = \int_0^1 \sum_{k=0}^{\infty} \frac{(-t)^k}{k!} t^{z-1} dt \tag{2.38}$$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \int_0^1 t^{k+z-1} dt = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!(k+z)} \tag{2.39}$$

(b) Beta function

In many cases it is more convenient to use the so called beta function instead of a certain combination of values of the gamma function. The beta function is usually defined by:

$$B(z, w) = \int_0^1 \Gamma^{z-1} (1-\tau)^{w-1} d\tau, (\text{Re}(z) > 0, \text{Re}(w) > 0). \tag{2.40}$$

To establish the relationship between the gamma function and the beta function we will use Laplace transform.

Let us consider the following integral

$$h_{z,w}(t) = \int_0^1 \Gamma^{z-1} (1-\tau)^{w-1} d\tau. \quad 2.41$$

Obviously, $h_{z,w}(t)$ is a convolution of the functions t^{z-1} and t^{w-1} and $h_{z,w}(1) = B(z, w)$.

Because the Laplace transform of a convolution of two functions is equal to the product of their Laplace transforms, we obtain:

$$H_{z,w}(s) = \frac{\Gamma(z)}{s^z} \cdot \frac{\Gamma(w)}{s^w} = \frac{\Gamma(z)\Gamma(w)}{s^{z+w}}, \quad 2.42$$

Where $H_{z,w}(s)$ the Laplace transform of the function $h_{z,w}(t)$.

On the other hand, since $\Gamma(z)\Gamma(w)$ is a constant, it is possible to restore the original function $h_{z,w}(t)$ by the inverse Laplace transform of the right hand side, we therefore obtain:

$$h_{z,w}(t) = \frac{\Gamma(z)\Gamma(w)}{\Gamma(z+w)} t^{z+w-1}, \quad 2.43$$

and taking $t=1$ we obtain the following expression for the beta function:

$$B(z, w) = \frac{\Gamma(z)\Gamma(w)}{\Gamma(z+w)}, \quad 2.44$$

from which it follows that

$$B(z, w) = B(w, z). \quad 2.45$$

$$h_{z,w}(t) = B(w, z) t^{z+w-1}.$$

(c) *Fractional Derivation*

Following approximation are use, arising from Grunwald-Letnikov definition:

$${}_a D_t^\alpha f(t) \approx {}_a \nabla_h^\alpha f(t).$$

Transition from $\alpha = 0$ to $\alpha = 1$, for which we obtained conventional first –order derivatives. Derivatives of the Heaviside function and the cosine function are unbounded at $t=0$. This is in agreement with the well-known asymptotic of the Riemann-Liouville fractional derivative of a function which is non-zero (but bounded) at the initial point $t=0$.

- **Trigonometric function**

Mittag-Leffler function plays an important role in the solution of fractional order differential equations. One of Mittag-Leffler function is exponent function, e^z , plays a very important role in the theory of integer-order differential equations. It's one parameter generalization, the function which is denoted by

$$E_\alpha(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)} \quad 2.46$$

(a) **Related Functions**

A two parameter function of the Mittag-Leffler type is defined by the series expansion.

$$E_\alpha(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + \beta)} (\alpha > 0, \beta > 0). \quad 2.47$$

It follows from the definition that

$$E_{1,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+1)} = \sum_{k=0}^{\infty} \frac{z^k}{k!} = e^z, \quad 2.48$$

$$E_{1,2}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+2)} = \sum_{k=0}^{\infty} \frac{z^k}{(k+1)!} = \frac{1}{z} \sum_{k=0}^{\infty} \frac{z^{k+1}}{(k+1)!} = \frac{e^z - 1}{z},$$

$$E_{1,3}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(k+3)} = \sum_{k=0}^{\infty} \frac{z^k}{(k+2)!} = \frac{1}{z^2} \sum_{k=0}^{\infty} \frac{z^{k+2}}{(k+2)!} = \frac{e^z - 1 - z}{z^2},$$

For $\beta=1$ we obtain the Mittag-Leffler function in one parameter:

$$E_{\alpha,1}(z) = \sum_{k=0}^{\infty} \frac{z^k}{\Gamma(\alpha k + 1)} \equiv E_{\alpha}(z). \quad 2.49$$

The function $\xi_t(\nu, a)$, introduced for solving differential equations of rational order, is a particular case of the Mittag-Leffler function

$$\xi_t(\nu, a) = t^{\nu} \sum_{k=0}^{\infty} \frac{(at)^k}{\Gamma(\nu + k + 1)} = t^{\nu} E_{1, \nu+1}(at). \quad 2.50$$

The following functions are particular cases of the Mittag-Leffler function in two parameters:

(b) Fractional Sine

Sine which can be expressed in terms of the Mittag-Leffler function as follows:

$$\sin_{\lambda, \mu}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{\Gamma(2\mu k + 2\mu - \lambda + 1)} = z E_{2\mu, 2\mu - \lambda + 1}(-z^2) \quad 2.51$$

(c) Fractional Cosine

Cosine which can be expressed in terms of the Mittag-Leffler function as follows:

$$\cos_{\lambda,\mu}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n}}{\Gamma(2\mu n + \mu - \lambda + 1)} = E_{2\mu, \mu - \lambda + 1}(-z^2) \quad 2.52$$

(d) *Generalized sine and cosine*

The fractional sine and cosine are particular cases of the Mittag-Leffler function in two parameters:

$$Sc_{\alpha}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{(2-\alpha)n+1}}{\Gamma((2-\alpha)n+2)} = zE_{2-\alpha,2}(-z^{2-\alpha}) \quad 2.53$$

$$Cs_{\alpha}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n z^{(2-\alpha)n}}{\Gamma((2-\alpha)n+1)} = E_{2-\alpha,1}(-z^{2-\alpha}) \quad 2.54$$

2.5 Watermarking techniques using 3D image representation DIBR

With the advancement of 3D viewing technology there is no doubt that the 3D space vision will be the choice for the future communication (devices). 3D visualization has been used in so many different areas such as from entertainment industry to scientific visualization, from medical to space area imaging etc. Protecting the contents of the 3D images is challenging task. In recent year many researchers are trying to develop new algorithms to protect intellectual property and ownership rights of original 3D scene/object. According to (Smolic et al., 2007) 3D watermarking schemes can broadly be divided into three types. In the first kind of 3D watermarking scheme, watermark is embedded and extracted in 3D space. In the second type, watermark embedding is performed in 3D space while watermark extraction is done in 2D space. This 2D space is actually a projection of 3D scene, geometry or structure. In the third kind, watermark embedding is performed in sequence of 2D images, which are 2D projections of a 3D scene. Watermark extraction is performed from the rendered 2D images. The third type

of 3D watermarking system has turn out to be more popular approach to protect 3D contents from being illegitimately circulated.

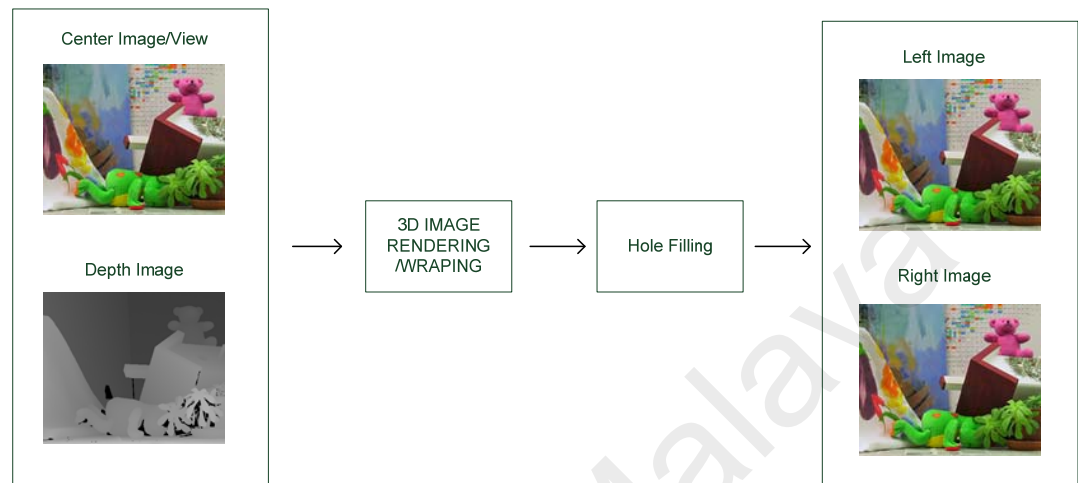


Figure 2.5: Depth image base rendering procedure.

The human visual ability to perceive depth of 3D scenes depends on different kinds of depth cues. There are mainly two kinds of depth estimation cues, monocular and binocular. Monocular provide depth information by one eye using different cues such as focus, defocus(blurring effect due to non-focus), texture gradient feature(edge direction), occlusion(overlapping), Aerial perspective(atmosphere haze), relative or absolute size or height of object, linear perspective, light and shading, motion(movement parallax) cues. Binocular provide depth information by taking input from both eyes. HVS perceive the depth component of the image by using binocular cues. Binocular cues involve fusion of two views perceived by the two eyes into single 3D view. Usually there are two main types of 3D image representation. The first type is stereo image. Stereo image consist of left eye image and right eye image. The second type consists of DIBR 3D image. DIBR have a center image and a depth image as shown in Figure 2.5.

2.5.1 Multi-dimensional discrete wavelet transforms

3D DWT is an example of multidimensional discrete wavelet transform. The 3D DWT can be visualized as an arrangement of three 1D DWT in the x, y and z directions. After a one-level of 3D discrete wavelet transform, the volume of image is decomposed into one low pass sub-band signal and seven high pass sub-bands such as HHH, HHL, HLH, HLL, LHH, LHL, LLH and LLL signals as shown in Figure 2.6.

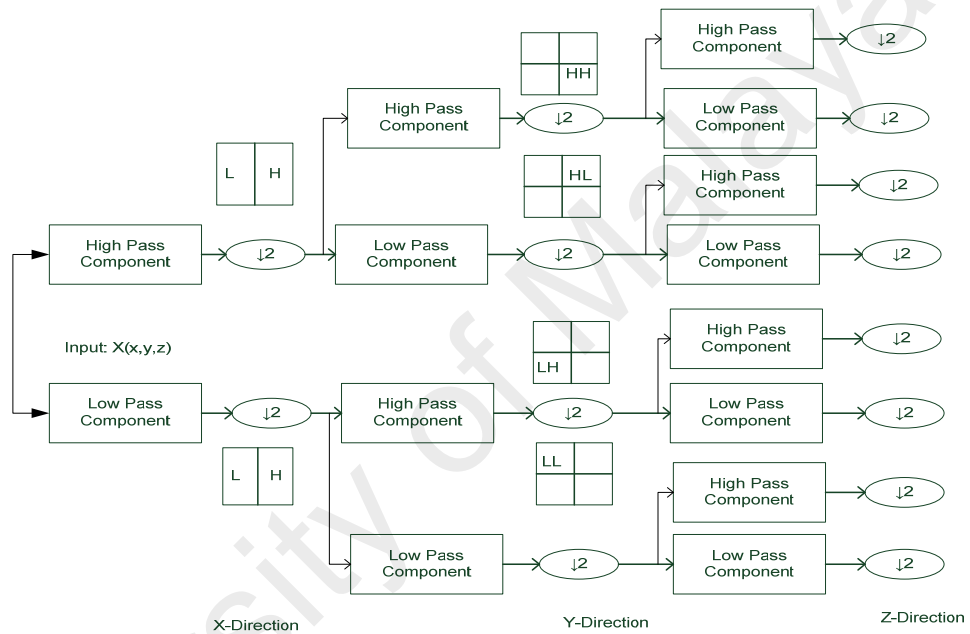


Figure 2.6: One-level 3D DWT structure (Tripathy, Sachdeva, & Talhi, 2009)

2.5.2 Related work

In literature stereo image based watermarking techniques has been proposed and very little work has been done in the watermarking DIBR 3D image Representation although the work on the 3D DIBR watermarking is more popular.

(D.-C. Hwang, Bae, Ko, & Kim, 2005) proposed a Discrete Wavelet Transform (DWT) and feature based window matching (FMA) algorithm for watermarking. Disparity data Comprised of difference between left stereo image and watermark right

image is calculated. The left stereo image along with disparity data is transmitted through communication channel. FMA algorithm uses the left stereo image and the disparity data to reconstruct the right image. Watermark is extracted using the difference between original and watermark right image. The drawback of this technique is that it is non-blind technique.

The author (Chammem, Mitrea, & Prêteux, 2011) proposed two methods to get a trade-off between transparency and robustness. They tried to design an algorithm which has low computational cost. A watermarking scheme based on adaptive disparity matching is proposed by (D. C. Hwang, Bae, & Kim, 2004). Right image is decomposed into second and third levels DWT. A watermark image of size 64×64 pixels is embedded into these DWT coefficients. The disparity data is computed from watermark right and left image. The derived disparity data and left image are transmitted through communication channel. From left image and disparity data watermark right image is reconstructed using adaptive matching algorithm based on the difference between the watermark right image and the original, right image. The embedded watermark image extracted from the reconstructed right image.

(Bhatnagar, Kumar, Raman, & Sukavanam, 2009) proposed a robust fractional Fourier transform (FrFT) and Singular Value decomposition based stereo image watermarking technique. Right disparity map is calculated using left and right stereo images and is used as watermark while left stereo image is used as host image. The host image is degraded by using zigzag sequence and then FrFT is applied to the degraded image. Watermark is embedded to the SVD value of the degraded image.

The authors in (S. Wang, Cui, & Niu, 2014) proposed SIFT feature selection based watermarking technique in DCT domain for DIBR 3D images for copyright protection of

the center, left and right images. They select stable feature points in circular area, in the center image to achieve robustness and imperceptibility. The feature points in the left, right images are determined using SIFT match by taking into account the information of features location and size. The proposed technique was robust just against JPEG attack and Median filter attacks. In (H.-D. Kim, Lee, Oh, & Lee, 2012), the author proposed robust block based watermarking technique for DIBR 3D images using DT-CWT (dual tree complex wavelet transform). They use third level of DT-CWT to embed the watermark. They exploit shift invariance and direction selectivity property of DT-CWT to embed the watermark imperceptibly. The experimental results shows that they achieve low Bit Error Ratios for the different signal processing and geometric attacks.

2.6 Chapter Summary

Digital image watermarking is a technique that aims to embed information called watermark in an image in such a way that the difference between the original and processed images is hardly noticeable. Digital watermarking is a mean to effectively deal with copyrights and ownership issues, access control and broadcast monitoring.

This chapter describe the basics of digital watermarking, watermarking requirements, watermarking applications and watermarking domains. Two key properties which are compliment to each other, should be considered while designing a watermarking system are robustness and imperceptibility. Further we also discussed the potential set of watermark attacks. Along with that the key topics discussed are perceptual modelling of watermark based on Artificial Intelligence (AI) techniques such as GP, IT2FLS, and RST invariant domain. Additionally polynomial domain based robust watermarking techniques and 3D DIBR techniques are also discussed.

Basic concept and related work are presented in this chapter. These discussion expose the gap in the watermarking methods. GP based watermarking technique for dynamic block size are proposed in the chapter 3. Distortion induced mainly due to geometric attacks such as RST attack is remain one of major challenge. We have tried to deal with it by proposing new watermarking domains. Which are discussed in chapter 4, 5. Finally we also deal with robustness issue of watermark in 3D DIBR images. Which is discussed in chapter 6.

CHAPTER 3: GENETIC PROGRAMMING FOR PERCEPTUAL MODELLING WITH DYNAMIC BLOCK SIZE

In this chapter we propose a dynamic block size watermarking technique. The proposed technique uses GP to generate perceptual mask of gray scale images in DWT domain. In this work, GP is trained to embed imperceptible watermark using block sizes of 4, 8, 16, and 32. Therefore, the proposed technique can embed watermark in an image using any these block sizes. Perceptual significance of coefficients is calculated in the DWT domain to get high level of robustness. Coefficients selected for watermark embedding are scattered throughout the image, which makes it more robust. We employ JPEG2000 Perceptual Model, to embed watermark imperceptibly. Experimental results show significant improvement in the imperceptibility of watermark for different block sizes and considerable enhancement in the robustness under different attacks.

3.1 Methodology

Our algorithm embed watermark in 2D-DWT domain. It works in two phases: watermark embedding phase and watermark extraction phase. In watermark embedding phase, as shown in Figure 3.1, an image X is transformed to first level discrete wavelet and embedding is performed in horizontal and vertical sub-bands in the wavelet domain. LH and HL bands are divided into independent, non-overlapping $m \times m$ blocks, where m is an integer. We used HL, LH sub-band at second level of 2D-DWT for watermark embedding. The watermark is usually embedded in middle frequency part of the image. As changes made to low frequency part i.e., LL sub-band can easily be visible to human eye, while the high frequency part i.e., HH sub-band is more sensitive to compression and scaling operation. That's why HL, LH sub-band is used for watermark embedding.

In our technique, we set it to 4, 8, 16, and 32. Then, perceptual significance of each $m \times m$ block is calculated using the following formula (First & Xiaojun, 2007):

$$S = \sum_{i=1, j=1}^{i=m, j=m} H(i, j)^2 \quad 3.1$$

where H represent any block within the sub-band whose coefficients, i, j can be up to size defined by m. The sum of square of the selected coefficients in a block of size $m \times m$ is represented by S. Based on the value of S of equation 3.1, blocks in the sub-band are arranged in ascending order. From the sorted list of blocks, b numbers of blocks are selected for the watermark embedding. Watermark is embedded in the selected coefficients using the following equation:

$$X'[i, j] = X[i, j] + |\alpha| * W[i, j] \quad 3.2$$

where $X'[i, j]$ is the watermarked coefficient, $W[i, j]$ is the watermark generated by pseudo random sequence and α is the HVS based function and represents perceptual mask of the selected watermark embedding coefficient. GP takes the luminance and contrast masking value for each of the selected coefficient in the 4, 8, 16 and 32 size blocks and determines the optimum value of the watermark. Using user specified selection criteria, GP iterates specified number of times until it gets best strength of watermark for the selected coefficient, balancing both the imperceptibility and robustness. In this way we get genetic perceptual mask using GP for the whole image with different block sizes.

In watermark detection phase, it is assumed that the user has advance knowledge of all steps performed for embedding data. Correlation method is used for the watermark detection. In second phase, watermarked image X' is decomposed into single level 2-

dimensional wavelet transform (DWT2). The HL, LH sub-bands are divided into $m \times m$ blocks. Sum of squares of coefficients are determined and sorted into descending order.

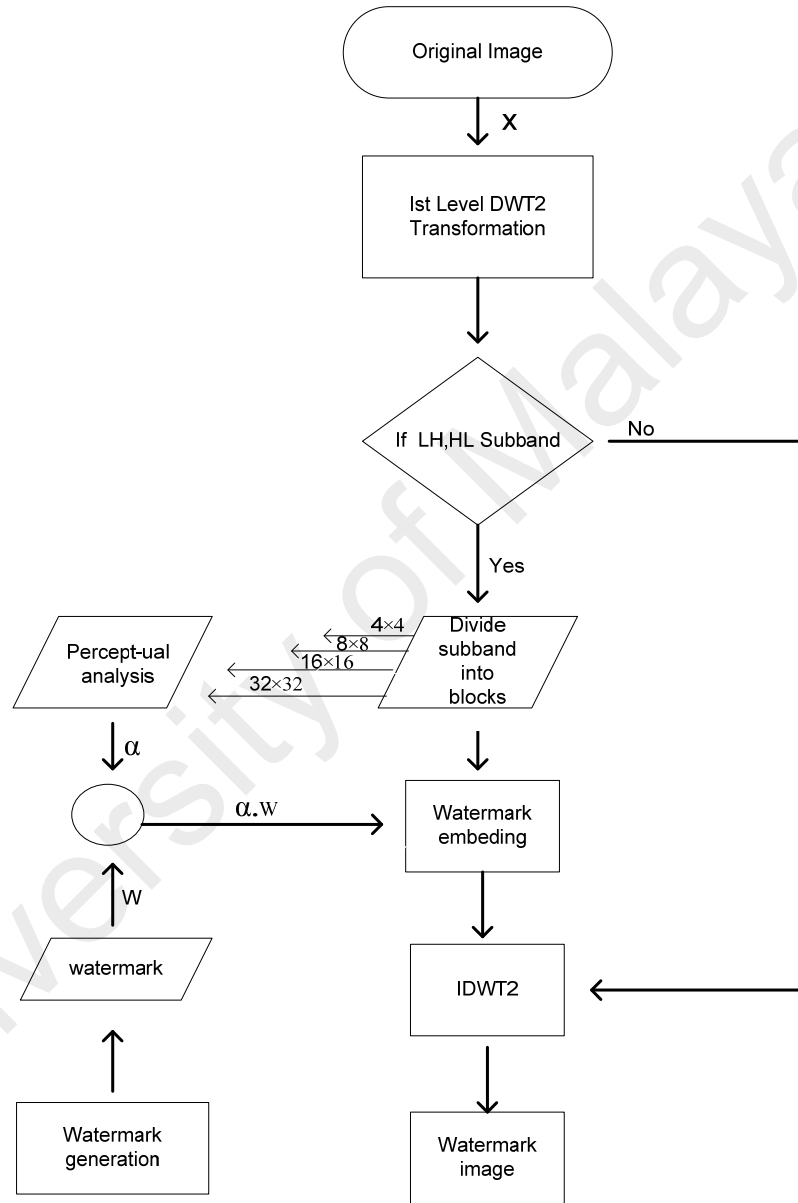


Figure 3.1: Dynamic block watermarking Technique flow diagram. Perceptual analysis part is performed by the GP.

From the sorted blocks, top b blocks are selected for the watermark detection purpose. The correlation between marked coefficient and the watermark is calculated using the equation

$$C = \frac{1}{M} \sum_{i=1}^M y_i \cdot t_i \cdot \alpha \quad 3.3$$

where M is the total number of coefficient to be marked, y_i is the watermark, t_i is the image coefficient to be marked and α is the watermark level calculated through GP. Finally, correlation value C is compared to predefined thresholds to determine whether the watermark exists or not.

3.2 Human Visual System (HVS)

A watermark is embedded using a perceptual model which exploits the characteristics of HVS to get the imperceptibility. In this technique, factors such as self-contrast masking, neighborhood contrast masking and luminance sensitivity are used. The strength of watermark which is to be embedded is control by HVS characteristics and in our technique is represented as:

$$\alpha = f(a_l(\lambda, \theta, i, j), a_c(\lambda, \theta, i, j)) \quad 3.4$$

$$a_c(\lambda, \theta, i, j) = a_{c_self}(\lambda, \theta, i, j) \cdot a_{c_neig}(\lambda, \theta, i, j) \quad 3.5$$

$$a_{c_self}(\lambda, \theta, i, j) = \max \left\{ 1, \left(\frac{|g(\lambda, \theta, i, j)|}{JND_{\lambda\theta} al(\lambda, \theta, i, j)} \right)^\varepsilon \right\} \quad 3.6$$

$$a_{c_neig}(\lambda, \theta, i, j) = \max\left\{1, \sum_{\kappa \in \text{neighbourhood}} \frac{\left(\left| \frac{\mathcal{G}(\kappa)}{JND_{\lambda\theta} al(\lambda, \theta, i, j)} \right| \right)}{N_{i,j}} \right\} \quad 3.7$$

where a_l represent luminance factor/variable while a_c represent contrast masking parameter, which can further be categorized as self-contrast masking and neighborhood contrast masking. For each DWT transformed coefficient, at location (i, j) within subband (λ, θ) where, λ is the transform level and θ is the orientation (Liu et al., 2006).

$$a_l(\lambda, \theta, i, j) = \left(\frac{\hat{\mathcal{G}}_{\lambda \max, LL_{i,j}}}{\hat{\mathcal{G}}_{mean}} \right)^{\alpha T} \quad 3.8$$

Now luminance masking is performed using equation 3.8, where $\hat{\mathcal{G}}_{\lambda \max, LL_{i,j}}$ is the coefficient value in LL sub-band that spatially corresponds to the location (λ, θ, i, j) . This parameter controls the degree to which luminance masking occurs and αT takes value of 0.649 as suggested in (Liu et al., 2006).

Contrast masking is performed using equation 3.5, where $a_{c_self}(\lambda, \theta, i, j)$ is self-contrast adjustment factor, while $a_{c_neig}(\lambda, \theta, i, j)$ is the neighborhood based contrast masking. The neighborhood consists of the coefficients in the same sub-bands that lie within a window centered at the location (i, j) , $N_{i,j}$ denotes the number of coefficients in that neighborhood, $\mathcal{G}(\lambda, \theta, i, j)$ is the DWT coefficient value at location (λ, θ, i, j) , and ξ is a constant that controls the influence of the amplitude of each neighboring coefficient.

For the LL sub-band, contrast masking is suppressed by setting $\epsilon = 0$. For other sub-bands, it is set to 0.6. Equation 3.6 and equation 3.7 performs the contrast masking. Just noticeable distortion (JND) threshold is formulated as specified in (Liu et al., 2006).

$$JND_{\lambda, \theta}(r) = \frac{1}{A_{\lambda, \theta}} a \cdot 10^k \left\{ \log_{10} \left(g_{\theta} f_0 2^{\lambda} / r \right) \right\}^2 \quad 3.9$$

Where a, g_{θ}, k, f_0 are constants, for the amplitude of the DWT 9/7 basis function corresponding to level λ and orientation θ , and r is the visual resolution of the display in pixels/degree. The values given in Table 3.1 and Table 3.2 are used for the above mentioned constants.

Table 3.1: Basic function amplitude $A(\lambda, \theta)$ for 1st level for a 9/7 dwt (Liu et al., 2006)

Orientation	DWT 1 st level decomposition
LL	0.62171
LH,HL	0.67234

Table 3.2: Parameters for DWT threshold model (Liu et al., 2006).

a	k	fo	gLL	gHL,gLH	gHH
0.495	0.466	0.401	1.501	1.0	0.534

An initial random population p is created by setting the parameter values as shown in Table 3.3. If b is the individual of this population and X is the image then for each

individual in the population, following steps are performed by GP to determine a GP expression for optimal strength of the embedded watermark. The algorithm is as follows:

1: Convert the image X into 1st level 2D-DWT.

2: If the LH or HL sub-band and then perform the following actions:

- a. Compute blocks each of size $m \times m$.*
- b. Compute sum of square of each coefficient in $m \times m$ block using equation 3.1.*
- c. Sort blocks in descending order and select top b blocks embedding.*
- d. Compute perceptual mask using equation 3.4.*
- e. Embed the watermark using equation 3.2.*
- f. Compute fitness using equation $\text{Fitness} = \text{Structure Similarity Index Measure (SSIM)}$.*
- g. Perform step2 for different block sizes 4, 8, 16, 32 to train the GP.*

There are two stopping criteria for the algorithm. One condition is that when the specified number of iteration is reached and the second is when the desired fitness value is achieved.

3.3 Experimental Results Discussion

MATLAB (Matrix Laboratory) is used for the implementation of the system with GP and GPLAB toolboxes. Standard images such as baboon, Lena, cameramen, airplane, Barbara of size 512×512 are used as cover images. Ramped half and half method defined in GPLAB is used to create initial population in GP. GP functions used include \sin , \cos , mylog , mydivide , \times , $-$, and $+$ to perform operation on variables and constants. Variable terminals include luminance, contrast masking and DWT coefficients. Random constants are used as constant terminals. When generations reach to the specified maximum number of generations or when program reaches the threshold fitness level, it terminates. The Fitness of individual is set to SSIM where SSIM is the Structure Similarity Index

Measure. Watson perceptual models JPEG2000, values for the first level are used for embedding purpose. Watermark embedding and watermark detection are performed on the images. All images used are gray scale of size 512×512. Watermarks are generated randomly and consist of real number. PSNR and MSE are used to calculate and evaluate the quality of the watermarked and distorted image.

Table 3.3: GP control parameters.

Objectives	GP parameters settings
Function set	+, −, ×, mydivide, mylog, sin, cos
Terminal set	Constant: random constants in range [-1 1] Variables: $(a_i(\lambda, \theta, i, j), a_c(\lambda, \theta, i, j))$, coef
Fitness	SSIM
Selection	Generational
Population size	300
Initial max depth	6
Initial population	Ramped half and half
Operator prob type	Variable
Sampling	Tournament
Expected no of off springs	Rank89
Survival mechanism	Keep best
Real max level	28
Termination	Generation 30

Attacks are performed in the MATLAB environment. We demonstrate the performance of the proposed scheme in term of robustness and fidelity. Figure 3.2 represent the PSNR and MSE values of the watermarked images with different block sizes of 4, 8, 16 and 32. It can be seen that PSNR value of all images, using different block sizes lies, well above 55 and for Barbara and airplane it reaches more than 60. It proves that our technique is equivalently good irrespective of the size of block chosen for embedding watermark. Whereas the MSE value for Lena image lies in the range 0.0309 to 0.0859, for the airplane the value lies in the range 0.0251 to 0.076, for the cameraman the MSE value lies in the range 0.0752 to 0.1295 and for the baboon the range is between 0.0331 to 0.057 for block size 4, 8, 16 and 32. When we compare the value of PSNR of cameraman and baboon, we see a comparatively high PSNR value for the baboon, for all block sizes. This is due to the high texture of the baboon image. We have used texture feature to imperceptibly embed the watermark (First & Xiaojun, 2007).

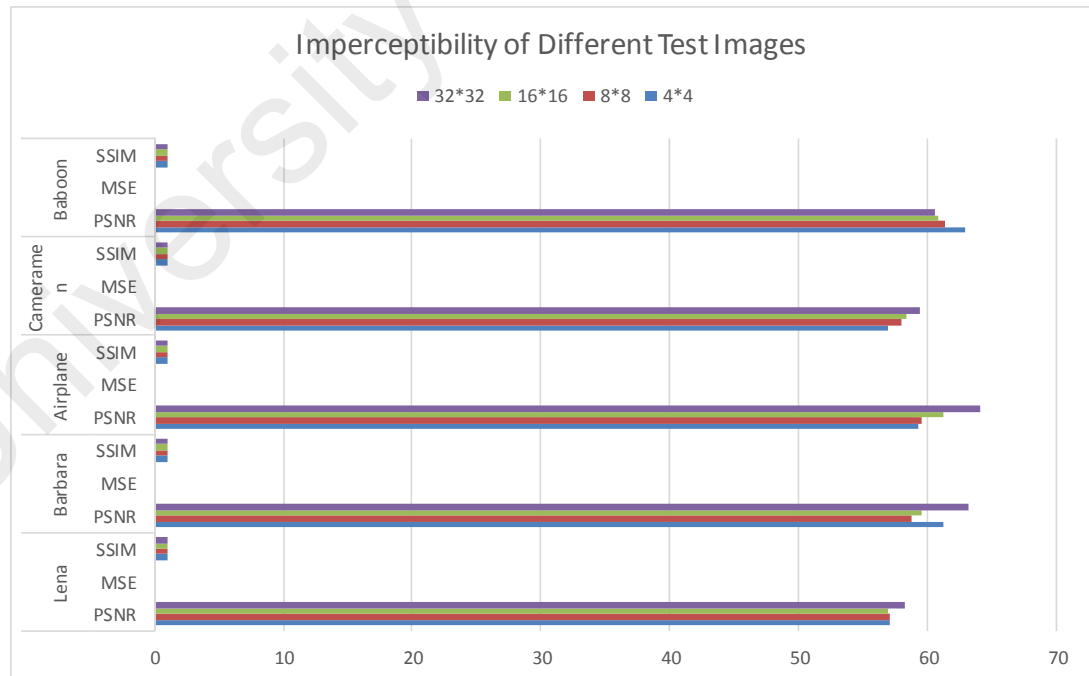


Figure 3.2: Comparison of imperceptibility of the proposed multi-block technique on different images with different block sizes.

Some common image processing operations such as filtering, compression, noise addition, rotation, cascading attacks are also applied to test the robustness of the proposed technique. Figures 3.3 to Figure 3.5 represent robustness level of the proposed technique against different types of attacks. Higher value of PSNR reflects the improved imperceptibility level of the watermarked image.

Table 3.4 compares the results of the proposed technique with the ones proposed in (Khan et al., 2006) and (Abbasi & Woo), labelled as Technique A and Technique B respectively, in terms of the quality of watermarked image, i.e., PSNR, MSE, and SSIM. The values in the column labelled “Proposed” in Table 3.4 show that our multi-block watermarking technique gives significantly better results than other two techniques. Figure 3.2 represents the comparison of PSNR, MSE, and SSIM values of different images using block size of 4, 8, 16, and 32.

Table 3.4: Comparison of cascading attack of varying strength, on image using different block sizes.

Type of attack	Attack value	PSNR			MSE		
		Technique A (Khan et al., 2006)	Technique B (Abbasi & Woo)	(Proposed)	Technique A (Khan et al., 2006)	Technique B (Abbasi & Woo)	(proposed)
low pass filter	2x2	21.86	37.18	39.61	81.47	12.44	7.12
	3x3	24.01	44.49	45.59	49.37	2.311	1.80
	4x4	20.41	37.18	39.61	112.37	12.44	7.11
	5x5	20.30	44.47	45.56	114.65	2.32	1.82

	6x6	18.65	37.18	39.61	166.67	12.45	7.11
G.noise	500	14.19	31.39	35.54	499	47.19	7.51
	1000	11.32	30.75	34.89	1002	54.76	3.42
	5000	05.46	29.68	32.62	5014	70.03	8.55
	10000	03.54	29.37	31.68	10014	75.23	6.85
	15000	02.64	29.23	31.26	15046	77.72	10.17
Median filter	2x2	21.61	37.10	39.37	86.33	12.68	7.51
	3x3	26.52	39.72	42.80	27.87	6.93	3.41
	4x4	20.84	36.43	38.80	102.45	14.46	8.55
	5x5	22.57	37.46	39.77	68.73	11.68	6.85
	6x6	19.61	35.87	38.06	135.44	16.81	10.17
Weiner jpeg & G.Noise	75,500	20.76	31.35	35.50	109.01	47.60	18.38
	50, 1000	18.54	30.73	34.86	185.0	54.98	21.23
	50,5000	12.12	29.67	32.61	842.0	70.19	35.67
	50, 1000	9.56	29.37	31.66	1612	75.17	44.36
	25,5000	12.59	29.65	32.59	752.0	70.47	35.84
	25,9000	10.08	29.40	31.79	1402	74.66	43.05
JPEG	100%	40.59	48.22	61.83	1.100	0.98	0.04
	75%	29.22	40.29	43.66	15.08	6.08	2.80
	50%	27.26	38.87	41.65	23.65	8.44	4.44
	25%	25.32	37.46	39.95	36.95	11.68	6.58
	10%	22.39	35.43	38.00	72.62	18.62	10.30

3.3.1 Filtering Attack

The watermarked image is attacked with a low pass filter, median filter with a window sizes from 2×2 to 6×6, and the Wiener filter. The watermark is detected after each attack

which shows our technique is robust to these types of attack as shown in Figure 3.3 and Figure 3.4.

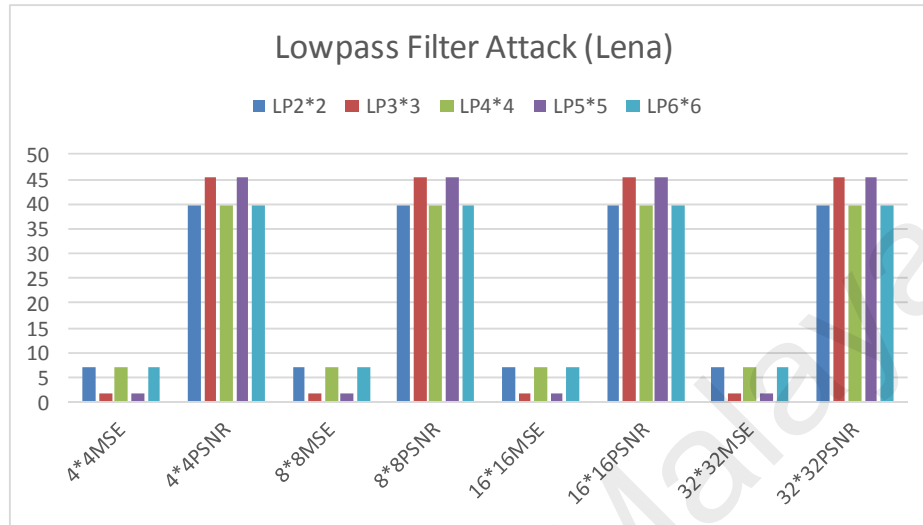


Figure 3.3: Comparison of PSNR and MSE values for the low pass filter attack on image using different block sizes.

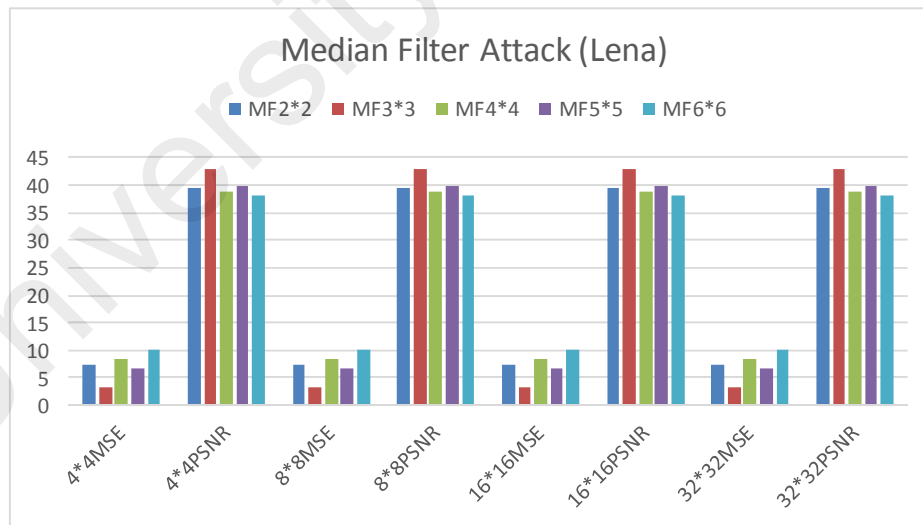


Figure 3.4: PSNR and MSE values for the median filtering attack of varying strength on images using different block sizes.

3.3.2 Noise Attack

The other type of attack carried out is Gaussian noise of window size 3×3 with standard deviation of 0.2. In addition, noise with power of 0.5k, 1k, 5k, 10k and 15k is added and the original watermark is detected from the attacked images (where k is 1000). The noise attack results are shown in Figure 3.5.

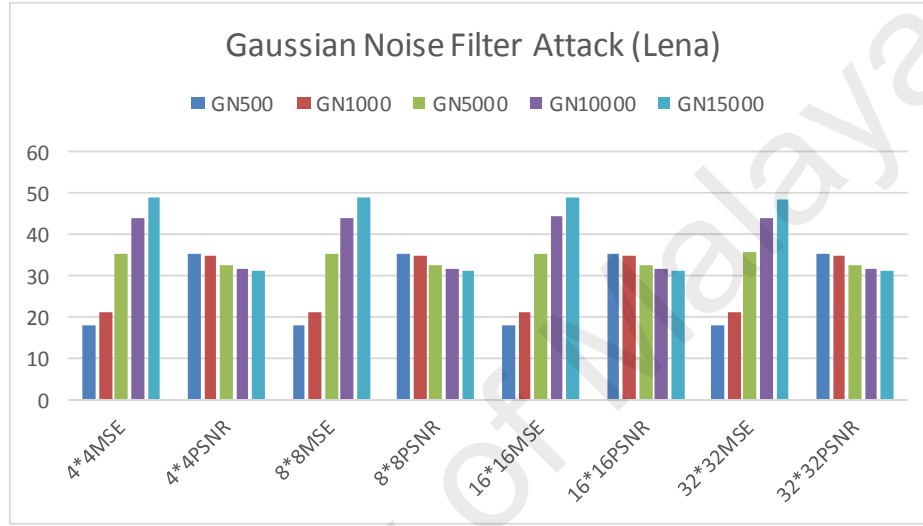


Figure 3.5: Comparison of adding Gaussian noise with different variance, such as 0.5k, 1k, 5k, 10k, 15k on image using different block sizes.

3.3.3 Compression Attack

Compression of watermarked images is performed with different JPEG quality values. The compression attack of different quality factor such as 75%, 50%, 25%, 10%, 7% and 5% is performed on set of images. For the Lena image the PSNR value for the block size 4, 8, 16, 32 are in the range 36.65 to 59.966, 36.65 to 39.38, 38.06 to 39.37 and 38.68 to 61.83 respectively for compression attack with Quality Factor (QF) 75%, to 5% . Watermark can still be detected after the compression attack with the quality factor as low as 5%.

3.3.4 Cascading Attacks

The image is also tested against cascading attacks. First, the image is subjected to Weiner filtering, and then the resultant image is compressed with different JPEG QFs such as 75%, 50%, 25%. We then add Gaussian noise with different variance such as 0.5k, 1k, 5k, and 10k in corrupt image. The detector was able to detect the watermark after each attack. The result of cascading attacks is shown in Figure 3.6.

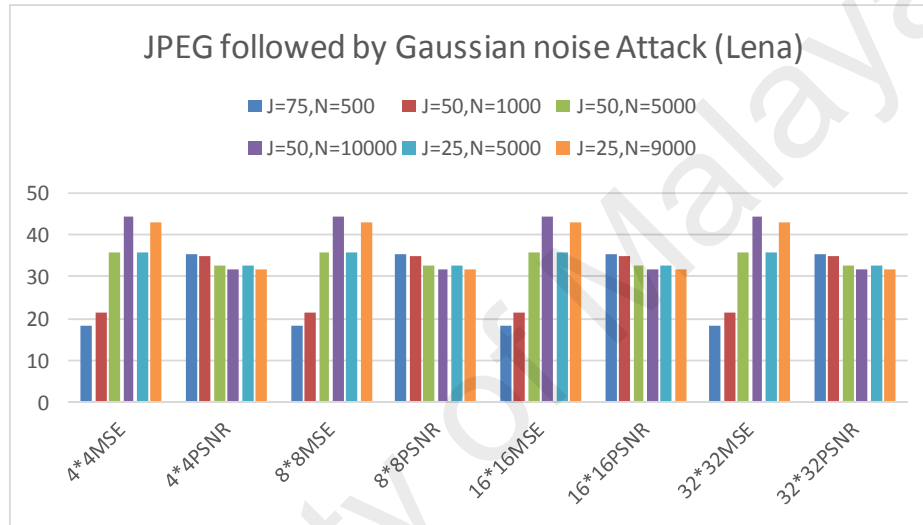


Figure 3.6: Comparison of JPEG attack of varying quality factors, together with Gaussian noise attack with different variance on images using different block sizes.

3.3.5 Geometric Attacks

In order to show the robustness against geometric attacks, cropping is used. Cropping with different rates (75%, 50%, and 15%) is applied. The watermark is also found to be robust against cropping attack. Watermark is also tested against the resize attack. A 512 × 512 image is resized to $\frac{1}{2}$ and $\frac{3}{4}$ of its original size. We were still able to detect the watermark. It indicates that our technique is robust against the resize attack.

3.4 Chapter Summary

In this Chapter i proposed a dynamic block watermarking technique. The proposed technique uses GP to generate perceptual mask of gray scale images in DWT domain. The novelty of the proposed technique is that it can embed watermark using any block size of an image.

The proposed technique intelligently offers a trade-off between robustness and perceptual changes that occur due to different set of malevolent attacks. Luminance sensitivity, self and neighborhood contrast masking of each coefficient are calculated and used to generate perceptual mask that is later used to determine optimal level of watermark for each of the selected coefficient in the block. The coefficients in which watermark is embedded are scattered throughout the image which makes it robust to different manipulations such as filtering attack, JPEG compression, adding noise, geometric and cascading attack etc. We have compared our dynamic block based technique with single block size technique presented in (Abbasi & Seng) and the genetic perceptual model based technique proposed in (Khan et al., 2006). We have compared PSNR value of attacked images and results show that our technique is 68% robust, while (Khan et al., 2006) and (Abbasi & Seng) are only 45% and 63% robust respectively. Experimental results indicate significant improvement in the fidelity of watermark for different block sizes and also considerable enhancement in the robustness under different attacks.

To effectively deal with the geometric attacks especially RST attacks we focus on invariant domains. In the next chapter we are proposing watermarking technique in RT domain.

CHAPTER 4: INVARIANT DOMAIN WATERMARKING USING RIESZ TRANSFORMATION

Conventional digital image watermarking techniques are often vulnerable to geometric distortions such as RST. These distortions desynchronize the watermark information embedded in an image and thus disable watermark detection. To address this problem, i propose an RST invariant watermarking technique using the RT, which has the properties of scale invariance, shift invariance and rotation invariance. The advantage of RST invariant domain is the elimination of resynchronization during watermark detection. Another advantage as compared with the majority of geometric invariant domain-based techniques is that the proposed watermarking technique is blind where watermark detection can be done without the original image. In the proposed method, watermark is embedded in all coefficients at the second scale for robustness. In addition IT2FLS is utilized for data fusion and building a model for spatial masking in the Riesz wavelet domain. Masking modeling is a complicated task and there is no single theoretical formulation to precisely compute the perceptual value for the corresponding wavelet coefficient. We compute the noise visibility, entropy and perceptual luminance values for each Riesz wavelet coefficients at the second order second scale. The computed noise visibility, entropy and perceptual luminance values are the fuzzy input variables, and the output of the fuzzy system is a particular value which gives a perceptual significance value for each corresponding Riesz wavelet coefficient. Cross correlation method based on Neyman-Pearson is deployed for watermark detection. Experimental results confirmed that the proposed technique has a good balance between robustness and imperceptibility under the checkmark tool.

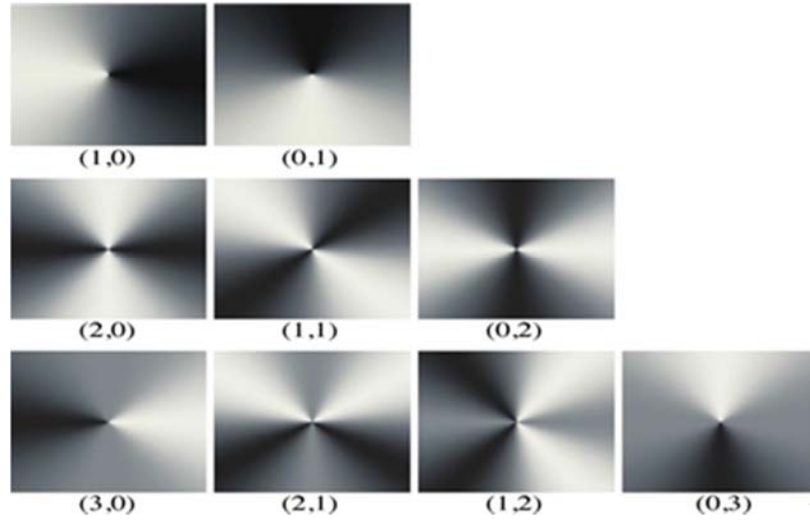


Figure 4.1: Frequency responses (real / imaginary part) of the components filters of the first, second and third order RT. The origin of the 2-D frequency domain is in the center and the intensity is stretched linearly for maximum contrast. (Unser & Van De Ville, 2010).

4.1 Methodology

We developed a watermarking technique in the invariant domain by exploiting the invariant properties of multidimensional RT as shown in Figure. 4.1. The geometric invariant domain also exploits the perceptual masking property of the Riesz wavelet to improve watermark fidelity. Furthermore, IT2FLS has been used to calculate the embedded watermark weight factor to balance between robustness and imperceptibility requirements of watermarking. Here, the weight factor of watermark is determined by using noise visibility, entropy and perceptual luminance values of the coefficients.

In this work, watermark is embedded in all coefficients of three subbands of second scale at order 2 of Riesz wavelet transformation. The following sub-sections detail the embedding and detection processes.

4.1.1 Watermark Embedding

Let $I(i, j)$ represent the original gray scale image of size $M \times N$ pixels and $w(i, j)$ is the watermark pattern to be embedded using additive embedding technique. Generally,

additive embedding is implemented by with using $I' = I + \alpha w$, where I' is the watermarked image, and α is the embedding strength. The size of the watermark w is equal to the size of the subbands selected for watermark embedding. All 3 subbands of Riesz Transformation coefficients at the second order, second scale are utilized for watermark embedding. The watermark embedding procedure has shown in Figure 4.3. The strength of watermark α for each coefficient is calculated by using IT2FLS, where α can be represented by the following equation:

$$\alpha(i, j) = f(nvf(i, j), e(i, j), l(i, j)). \quad (4.1)$$

Here nvf denotes the noise visibility function, e is the entropy of the image coefficients, and l the perceptual luminance. The values of nvf , l and e are calculated for all coefficients selected for watermark embedding, and these are the inputs to IT2FLS. We designed 99 fuzzy rules to take into account for all the possible combinations of the three inputs, which include NVF, entropy, and perceptual luminance. The rules are applied on each selected Riesz transform coefficient. This produces a watermark masking weight factor for each selected coefficient. The rules are in the form of

If (Condition1) and (Condition2) and (Condition3) then action,

where the action is adjusting the weight factor α by using IT2FLS based on the values of three inputs. The fuzzy rules are constructed using the following facts: Noise is more visible in flat area compared to texture region. In other words, higher the texture, higher the ability to hide noise. On the other hand, our eyes are less sensitive to the noise areas of the image where brightness are high or low. The watermark weight factor α is multiplied by the watermark and added to the coefficient, it is least visible. Thus it is an adaptive approach that fulfills the imperceptibility condition of watermarking depending

on the subband coefficients value of the image. The factors considered for calculating α using IT2FLS are shown in Figure 4.2.

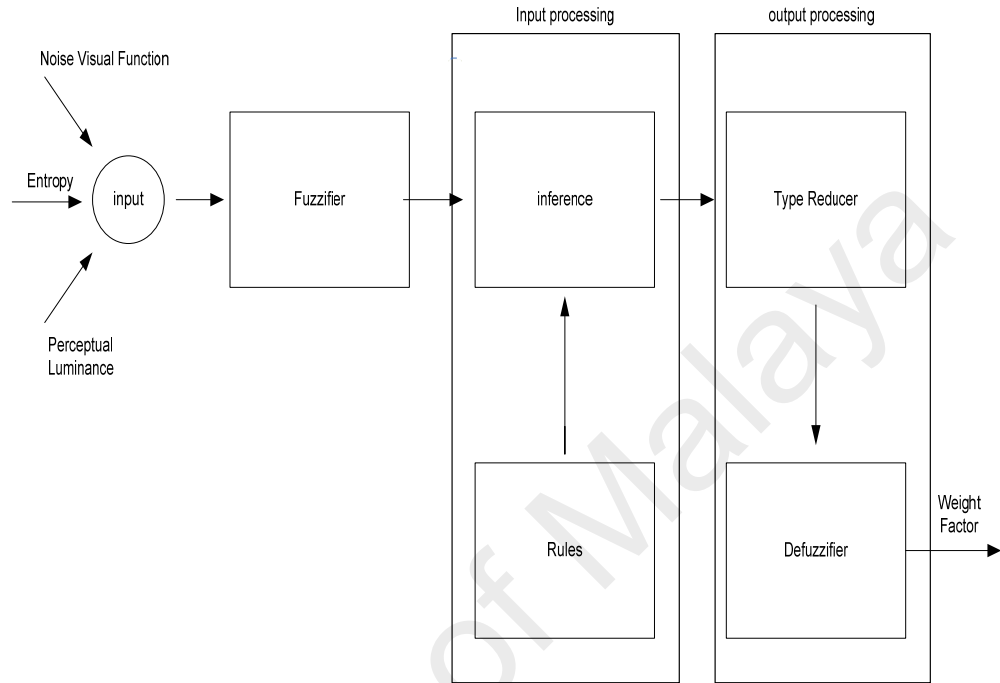


Figure 4.2: Overview of input and output of IT2FLS.

For the current implementation, the watermark signal is a sequence of +1 and -1. The watermark embedding process can be represented by the following equation:

$$S = s + (w_b \times w_p \times \alpha), \quad (4.2)$$

where S represents the watermark signal, s is the original signal (i.e. RT coefficients in our case), w_b is the watermark bit carrying the watermark message, and w_p denotes the reference pattern for hiding the watermark message. The parameter α is calculated using IT2FLS as expressed by equation. (4.1).

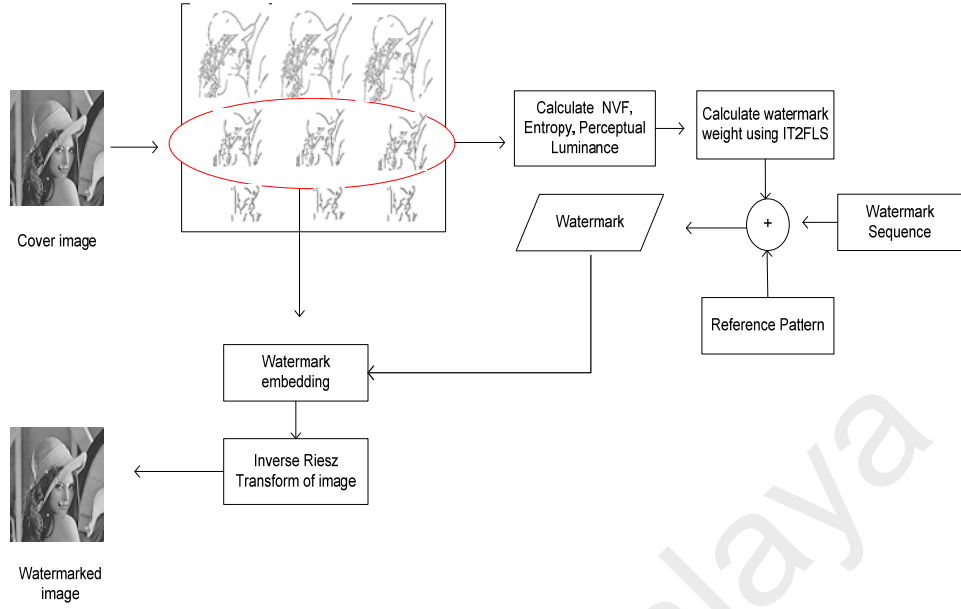


Figure 4.3: Process flow of the proposed technique.

4.1.2 Watermark Detection

Watermark detection is essentially the reverse of the embedding processes and it is shown in Figure 4.4. The correlation between the watermarked coefficient and the watermark to be tested for existence is computed using the following expression:

$$\rho = \frac{1}{MN} \sum_{\theta=0}^3 \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I_0^{\theta}(i, j) w^{\theta}(i, j), \quad (4.3)$$

where $I_0^{\theta}(i, j)$ is the RT subband coefficient and $w^{\theta}(i, j)$ represents the watermark pattern in the θ -th subband. The computed value of ρ is then compared to the threshold value T_{ρ} calculated using following equations:

$$T_{\rho} = 3.97 \sqrt{2\sigma_{\rho\beta}^2}, \quad (4.4)$$

where $\sigma_{\rho\beta}^2$ represents the variance and

$$\sigma_{\rho\beta}^2 \approx \frac{1}{(MN)^2} \sum_{\theta=0}^3 \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I_0^{\theta}(i, j))^2 \quad (4.5)$$

For the detailed derivation of these equations, we refer the interested readers to (Barni et al., 2001). The existence of the watermark will be confirmed when $\rho > Tp$.

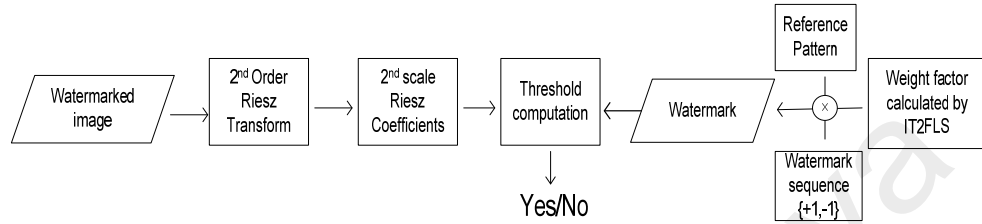


Figure 4.4 Watermark detection for the invariant domain

4.2 Experimental Results Discussion

In this section, we evaluate the performance of the proposed RT based watermarking technique by considering robustness and imperceptibility. Five standard test images from the USC-SIPI dataset, namely, Baboon, Cameraman, Lena, Peppers, and Sailboat, are considered for evaluation purposes. These images are each of dimensions 512×512 pixels and they are shown in Figure. 4.5(a-e). As a proof of concept, the algorithm is coded by using Matlab and checkmark (Shelby Pereira, 2001) is deployed for testing the robustness against different set of attacks. The watermark signal is represented by the sequence of +1 or -1, and the sign of samples are taken as the reference pattern.

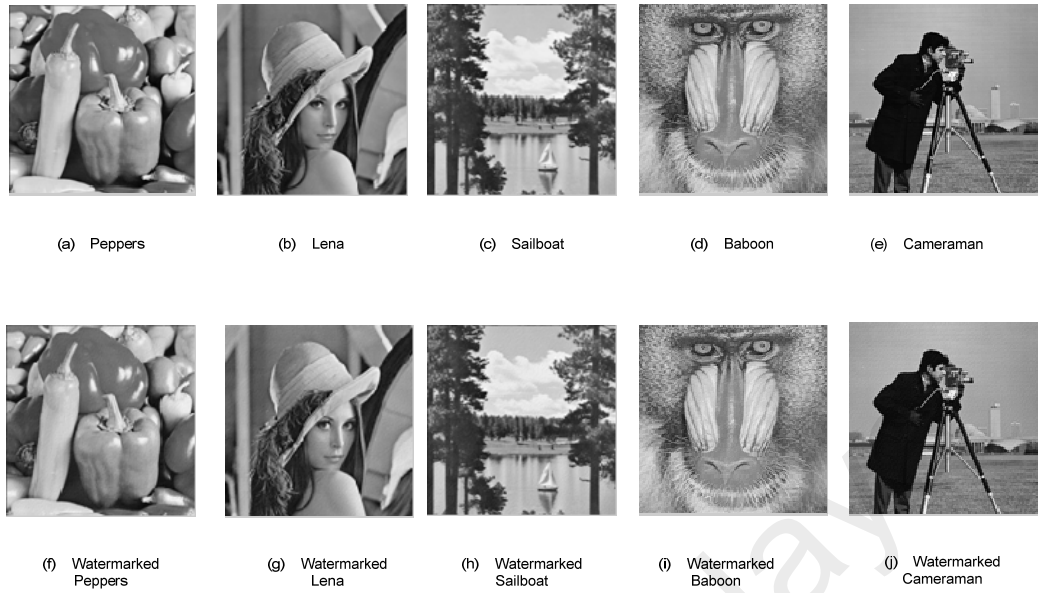


Figure 4.5: Original (a-e) and watermarked test images (f-j).

4.2.1 Imperceptibility

The watermarked images obtained by using the proposed technique are shown in Figure 4.5(f-j), where in each Image total 196,608 bits of watermark are embedded in each test image. By visual inspection, it is confirmed that the watermarked images appear perceptually similar to their original counterparts. To quantify the transparency of the embedded watermark, PSNR and SSIM (Z. Wang et al., 2004) are considered, which are commonly used by the watermark community. The results are recorded in Table 4.1. It is observed that the PSNR and SSIM values range from 41.20 to 42.71dB and 0.93 to 0.98, respectively. These readings suggest that the watermark image generated by the proposed method is of high perceptual quality.

Table 4.1: PSNR and SSIM value of watermarked images at second level of RT.

	Lena	Baboon	Cameraman	Sailboat Boat	Peppers
PSNR	41.85	41.74	42.71	41.63	41.20
MSE	4.24	4.35	3.49	4.47	4.93
SSIM	0.94	0.98	0.93	0.96	0.95

4.2.2 Robustness

Table 4.2 summaries the list of attacks performed on the watermarked image produced in our proposed technique. Cross correlation method based on Neyman-Pearson (Barni et al., 2001) is deployed to detect the embedded watermark using equation 4.3.

The watermarked images have undergone various types of attack to investigate the robustness of the proposed technique. In particular, each watermarked image is distorted using 10 different geometric and image processing attacks, namely: (1) rotation attack with angle θ ranges from -1 to 1 degree with step size of 0.25 degree and cropping scaling option; (2) rescaling attack with scaling factor ranging from 0.5 to 2; (3) translation attack with zero padding up to 1024 pixels along the x and y axes ; (4) JPEG compression with quality factor ranging from 10 to 90 with increment of 10; (5) row and column removal attack with the number of rows and column removal varying from 1 to 17; (6) change in aspect ratio in the x and y directions; (7) Gaussian filtering with kernel size of 3×3 and 4×4 pixels; (8) random bending attack; (9) shearing attack in the x and y directions, and; (10) sharpening attack.

Table 4.2: Performance of the proposed technique at second orders first, second and third scale of RT.

Attack Category	Description	Watermark Detection(5 images) Proposed Technique
Rotation	$\Theta = -1, -0, -0.75, -0.5, -0.25, 0.25, 0.5, 0.75, 0.90, 1.$ $\Theta = -0 \text{ to } 0.25. \text{ (Scale1)}$ $\Theta = -0 \text{ to } 0.75. \text{ (Scale2)}$ $\Theta = -1 \text{ to } 1. \text{ (Scale3)}$	1
Scaling	$0.5, 0.75, 0.90, 1.5, 2$ $0.5 \text{ to } 2.0. \text{ (All scales)}$	1
Translation 1	Circular shift $[1 -1], [-1 1] \text{ (Scale1)}$ Circular shift $[1 1], [1 -1], [-1 1], [-1 -1]$ (Scale2) Circular shift $[1 1], [-1 -1], [2 2], [-2 -2]$ (Scale3)	1

Translation 2	(0,1024),(1024,0) With zero padding (All scales)	1
Cropping	0% of image size. (Scale1) 1% of image size. (Scale2) 2% of image size. (Scale3)	1
JPEG Compression	<u>10,20,30,40,50,60,70,80,90</u> 10% to 90%. (All scales)	1
Random Bending	Random bending attack. (All scales)	1
Row and column removal	<u>1,2,3,4,5,6,7,.....17</u> Remove 1 to 17 rows and columns. (All scales)	1
Aspect Ratio Change	Change aspect ratio in x and y direction. (All scales)	1
Gaussian Filtering	Kernel size 3×3, 4×4. (All scales)	1
Shearing	Shearing in x and y direction. (All scales)	1
Sharpening	Unsharp filter. (All scales)	1

A score of 1.00 in the watermark detection column of Table 4.2 indicates that the watermark is detected in all images for the specified category of attack, while a 0.00 implies that no watermark is detected at all. For completion of discussion, the experimental results of subbands at second scale, second order of RT are also compared with other subbands, particularly, the first and third scale of second order. In general, the proposed technique achieves high robustness against the aforementioned attacks, which

is supported by the observed high cross correlation value against dynamic threshold. It is clear that the subbands at third scale of second order RT are more robust than that of other two subbands. This agrees with the theory, which says that robustness increase with the increase of scale level.

Next, we evaluated the performance of the proposed technique under the RST attack and the results are summarized in Figure 4.6(a-d). The cross correlation computation based on Neyman-Pearson criterion ρ and the threshold value T_ρ are considered to test the presence of the embedded watermark. The results for the rotation attacks with different angles ranging from -1 to 1 degree step size of 0.25 degree, followed by cropping and scaling operations are used as shown in Figure. 4.6(b). It is observed that the proposed method can survive the rotation attack. However, it is found that the proposed method is vulnerable to rotation attack when the magnitude of rotation goes beyond 1 degree.

On the other hand, the scaling attack using various factors ranging from 0.5 to 2.0, translation attack up to 1024 pixels i-e 2 rows and 2 columns along the x and y axis are applied to the watermarked image. In all cases considered, ρ remains well above the T_ρ threshold considered as suggested by Figure. 4.6(a) and Figure. 4.6(c-d). This is due to the properties of Resiz Transformation, which is translation and scaling invariant.

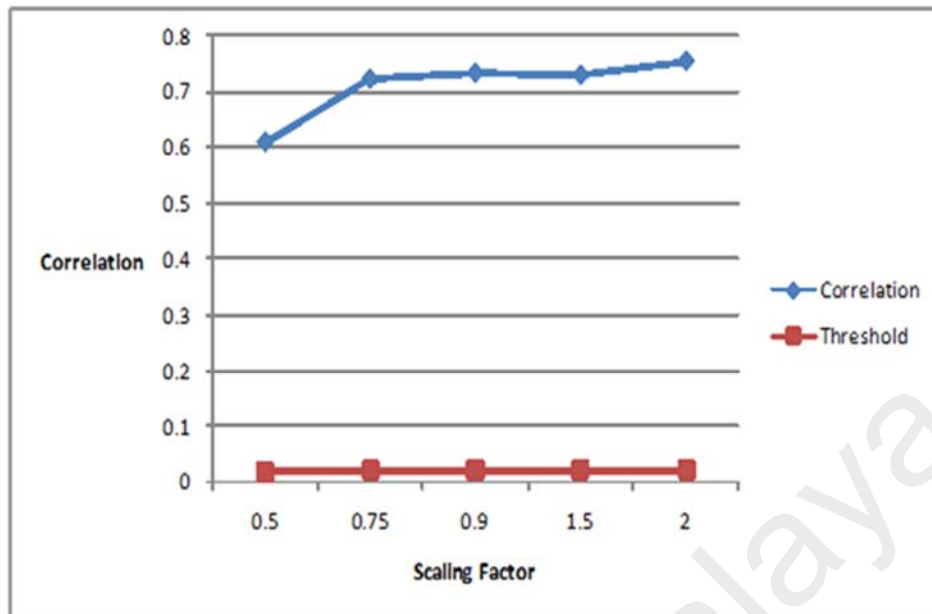
Robustness against JPEG compression with quality factor ranging from 10% to 90% and random bending attack are also evaluated. The presence of watermark is detected in all these cases. It should be noted that the random bending attacks desynchronize pixel location, but its effect is insignificant to our proposed technique due to the shift invariance property of RT, as suggested by the results recorded in Table 4.2.

Last but not least, common image processing operations such as cropping, median filtering, aspect ratio change, shearing and sharpening, linear transformation and Gaussian filtering are also applied on the watermarked image. For all cases, the dynamically computed ρ value always stays above the threshold T_ρ , i.e., 100% successful detection. The robustness of wavelet-based methods against these types of attack is due to their multi-scale and multi-resolution characteristics.

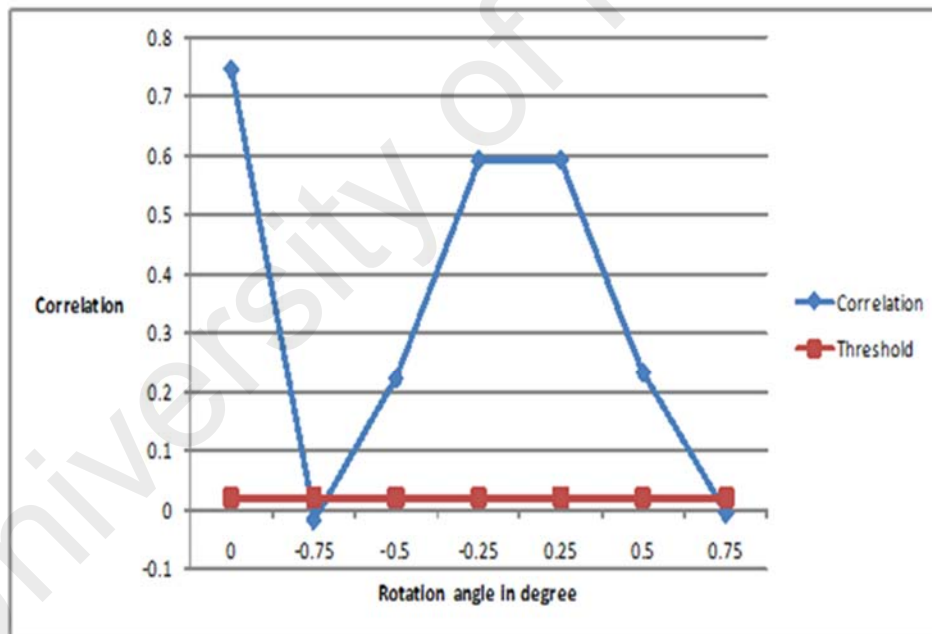
Therefore, the results suggest that the proposed method is robust against the commonly considered watermarking distortion attacks, with an exception of rotation attack for large angle.

To improve invariance against rotation attack we also developed a RST invariant domain using LPM and RT. LPM has been used for rotation invariance. LPM convert the image rotation operation into shift operation. In our technique the RT is shift invariant, this makes the combination of LPM and RT RST invariant. However since LPM result in visual quality degradation LPM and inverse LPM step of our proposed technique induce interpolation error. Figure 4.7 shows the results of improvement against rotation attack using LPM and RT. The watermark presence is detectable at rotation angle of up to 4 degree for the lena image as shown in Figure 4.7(a). Which proof that the LPM, RT is rotation invariant domain. Moreover further to increase the robust of the proposed technique against RST attack, specially rotation attack, quantization based method also proposed in (Abbasi , Woo & Shamshirband , 2015).

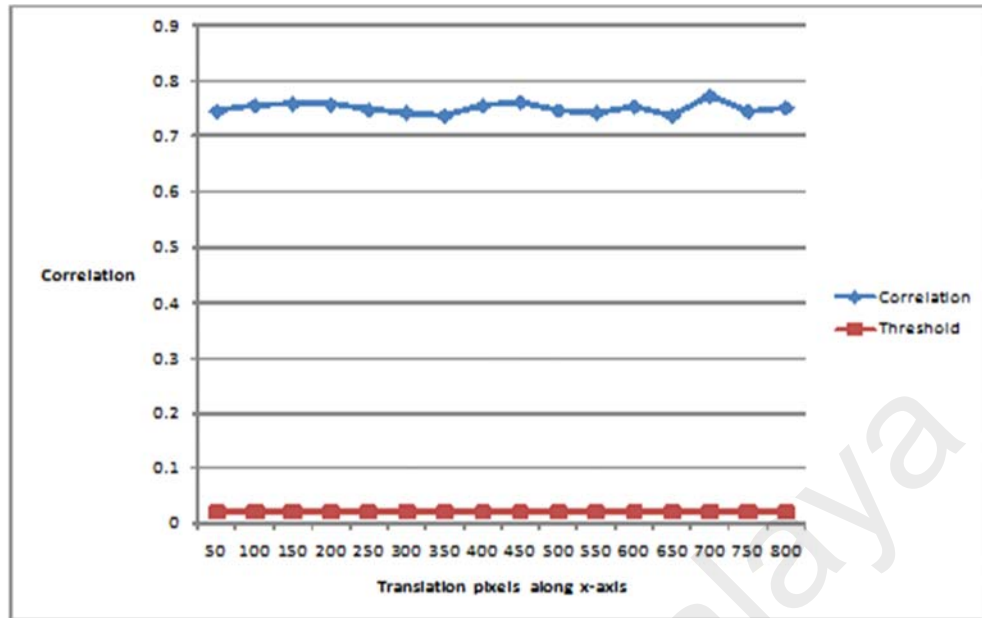
Further we successfully tested the proposed technique on a set of images (nearly above 1000 test image) acquired from image database (Gerald Schaefer Jun 2004).



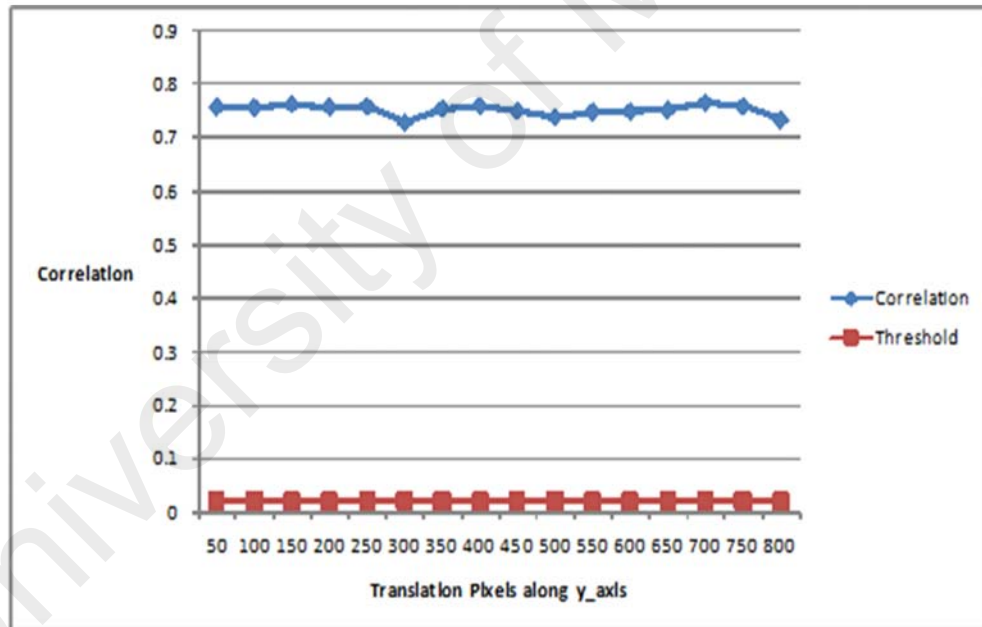
(a) Scaling Attack



(b) Rotation Attack

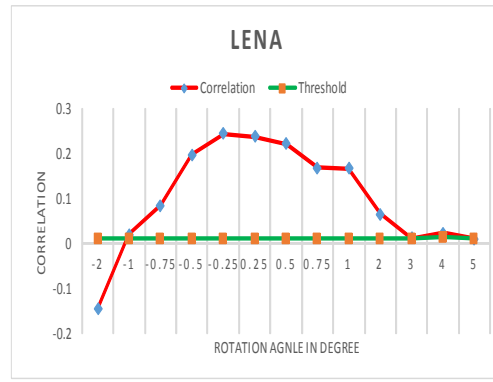


(c) Translation Attack zero padding along y-axis

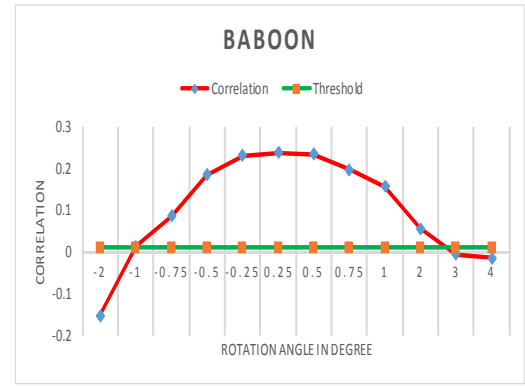


(d) Translation Attack zero padding along x-axis

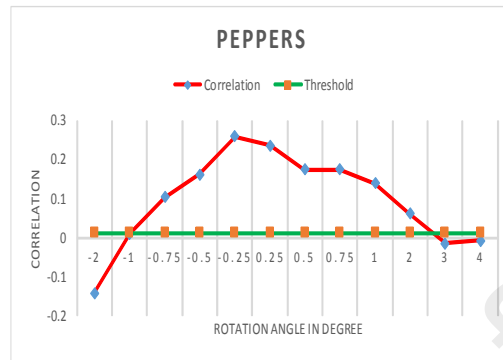
Figure 4.6: Robustness against RST attack at scale 2 of RT: Correlation in five test images: (a) Average correlation of five test images after scaling attack. (b) Average correlation of five test images after rotation attack. (c) Average correlation of five test images after translation attack zero with padding along y-axis. (d) Average correlation of five test images after translation attack zero with padding along x-axis.



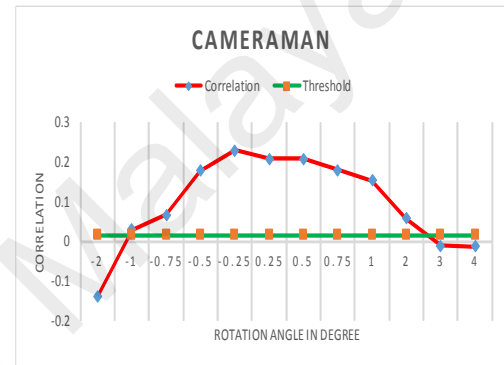
(a)



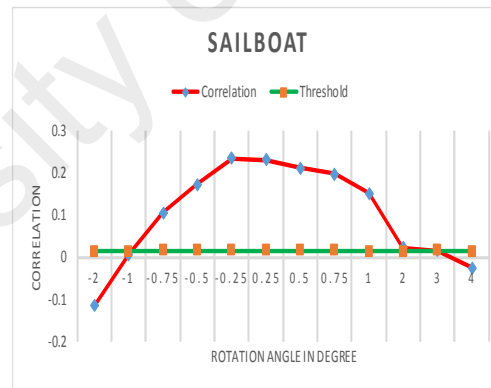
(b)



(c)



(d)



(e)

Figure 4.7: Robustness against rotation attack using LPM and RT of five test images

Table 4.3: Performance of the proposed technique and comparison of robustness test with other techniques.

Attack category	Description	Watermark Detection (3 images)		
		•	(Woo 2006)	Proposed Technique
Rotation	$\Theta = -1, -0.75, -0.5, -0.25, 0.25, 0.5, 0.75, 0.90, 1$ $\Theta = -1$ to 1	1	1	1
Scaling	$0.5, 0.75, 0.90, 1.5, 2$ 0.5 to 2.0	0.870	0.722	1
Translation 2	(0,1024),(1024,0) With zero padding	×	×	1
Cropping	2% of image size	1	1	1

JPEG Compression	<u>10,20,30,40,50,60,70,80,90</u> 10% to 90%	0.900	1	1
Random Bending	Random bending attack	0.950	1	1
Row and column removal	<u>1,2,3,4,5,6,7,.....17</u> Remove 1 to 17 rows and columns	×	1	1
Aspect Ratio Change	Change aspect ratio in x and y direction	×	1	1
Gaussian Filtering	Kernel size 3×3,4×4	×	1	1
Shearing	Shearing in x and y direction	×	1	1
Sharpening	Unsharp filter	×	1	1

4.2.3 Comparison with Existing Methods

There are very few works on global invariant domain for robust watermarking. A direct comparison with similar work is made here involving Kim et al.'s method (H. S. Kim & Lee, 2003) and Woo et al.'s method (Woo et al., 2006). To fairly evaluate the methods, the same set of attacks is applied to the watermark images generated by (Woo et al., 2006) and (H. S. Kim & Lee, 2003). The experimental results recorded in Table 4.3 confirm that our proposed technique has good level of robustness while maintaining good fidelity.

For scaling attack, our technique achieved 100% detection while (H. S. Kim & Lee, 2003) and (Woo et al., 2006) yield 87% and 72% detection, respectively. For translation attack with zero padding, no result was reported in (H. S. Kim & Lee, 2003), but (Woo et al., 2006) and the proposed method both achieve 100% detection.

For the JPEG compression and random bending attacks, Kim et al.'s method yields 90% and 95% detection, respectively, while Woo et al.'s method and the proposed method achieve 100% for both attacks. For the other types of geometric attack such as row column removal attack, aspect ratio attack, linear transformation attack, Gaussian filtering attack, sharpening and shearing, both Woo's method and the proposed method achieve 100% detection, but the aforementioned attacks are not considered in Kim et al.'s method.

With the aforementioned observations, we conclude that the proposed method performs better than the conventional RST invariant watermarking methods considered.

4.3 Chapter Summary

A RT based watermarking technique was proposed to exploit the wavelet based RT properties in developing a RST invariant domain. The multi-scaling and multi-resolution characteristics of wavelet based RT result in an increase in robustness against common watermark attacks. IT2FLS is utilized to calculate the dynamic watermarking weight factor for all the coefficients selected to embed watermark with less distortion while maintaining robustness. Since RT is RST invariant, the proposed domain does not require the resynchronization step in the watermark detection process, unlike the majority of the invariant domain based techniques. In addition, our technique is blind, which eliminates the need of the original image in watermark detection. Experimental results confirmed that the proposed technique has a good balance between robustness and imperceptibility, and it outperforms the conventional RST watermarking methods considered.

In next chapter we explore two new fractional Calculus based watermarking domain to achieve geometric invariance.

CHAPTER 5: INVARIANT DOMAIN WATERMARKING USING FRACTIONAL CALCULUS

Theory of derivatives and integral involving real order of complex order has its significance in different areas such as computer science, engineering and physics (mathematical). It generalized the concepts of integer order differentiation and n-fold integration. Fractional derivatives present a wonderful tool for the explanation of general properties of several processes such as signal processing and image processing. This is one of the core advantage of fractional derivatives in contrast with classical integer-order models, in which small effects detail are usually ignored (Jalab & Ibrahim, 2012), (Ibrahim, 2013). Detail of the fractional calculus and its special functions are given in Chapter 2. One of these famous operators in fractional calculus are the Riemann-Liouville operator (differential and integral), which defined by

Definition 5.1. The fractional (arbitrary) order integral of the function of order $\alpha > 0$ is defined by

$$I_a^\alpha f(t) = \int_a^t \frac{(t-\tau)^{\alpha-1}}{\Gamma(\alpha)} f(\tau) d\tau. \quad 5.1$$

Definition 5.2. The fractional (arbitrary) order derivative of the function of order $0 < \alpha < 1$ is defined by

$$D_a^\alpha f(t) = \frac{d}{dt} \int_a^t \frac{(t-\tau)^{-\alpha}}{\Gamma(1-\alpha)} f(\tau) d\tau = \frac{d}{dt} I_a^{1-\alpha} f(t). \quad 5.2$$

Remark 5.1. From Definition 5.1 and Definition 5.2, we have

$$D^\alpha t^\mu = \frac{\Gamma(\mu+1)}{\Gamma(\mu-\alpha+1)} t^{\mu-\alpha}, \mu > -1; 0 < \alpha < 1 \quad 5.3$$

$$I^\alpha t^\mu = \frac{\Gamma(\mu+1)}{\Gamma(\mu+\alpha+1)} t^{\mu+\alpha}, \mu > -1; \alpha > 0. \quad 5.4$$

In our investigation, we utilize the sinc and Heaviside basis functions.

5.1 Sinc Function

The sinc function, also known as the "sampling function," is a function that arises often in theory of Fourier transforms and signal processing.

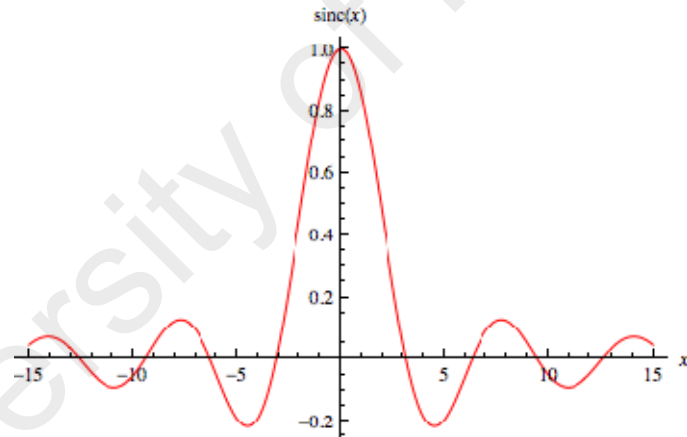


Figure 5.1: The sinc Function (Weisstein, 2014b)

Definition 5.3. The function $\text{sinc}(t)$ defined by

$$\text{Sinc}(t) = \frac{\sin(t)}{t}, \quad t \neq 0 \quad 5.5$$

For fractional $\text{Sinc}(t)$ of order α , (Sc_α), defined by (Podlubny, 1999)

$$Sc_{\alpha}(t) = \frac{\sin_{\alpha}(t)}{t} \\ = \sum_{n=0}^{\infty} \frac{(-1)^n t^{(2-\alpha)n+1}}{\Gamma((2-\alpha)n+2)},$$

Where $\sin_{\alpha}(t) = \sum_{n=0}^{\infty} \frac{t^{n-\alpha}}{\Gamma(n-\alpha+1)} \sin((n-\alpha)\frac{\pi}{2})$, Γ is the gamma function, t is

the variable and $\alpha \in (0,1)$ is a constant. From Definition 5.3, we have the following coefficients

$$\begin{aligned} \phi_0 &= \frac{1}{\Gamma(2)} \\ \phi_1 &= \frac{(-1)}{\Gamma(4-\alpha)} \\ \phi_2 &= \frac{1}{\Gamma(6-2\alpha)} \\ &\vdots \\ \phi_n &= \frac{(-1)^n}{\Gamma((2-\alpha)n+2)} \end{aligned}$$

Properties of sinc

1. Normalization:

$$\int_{-\infty}^{\infty} \text{sinc}(x) dx = \pi$$

2. Fourier transform of sinc function:

$$F(\sin c) = \Pi(t) = \begin{cases} 1, t > 1/2 \\ 1/2, t = 1/2 \\ 0, t < 1/2 \end{cases}$$

3. Inverse Fourier transform of sinc function

$$F^{-1}(\text{Sinc}) = \frac{1}{\pi} \text{Sinc}(t)$$

5.2 Heaviside Function

The Heaviside also called the unit step function, usually denoted by H (but sometimes u or θ), is a discontinuous function which take a value one for positive argument and zero value for negative argument. It rarely concern what value is used for $H(0)$, since H is frequently used as a distribution.

The function is used in the mathematics of control theory and signal processing to represent a signal. It is also used in structural mechanics along with the Dirac delta function to designate different kinds of structural loads.

The Heaviside function is the integral of the Dirac delta function: $H' = \delta$. it can be written as:

$$H(x) = \int_{-\infty}^x \delta(s) ds \quad 5.7$$

Though this extension may not hold (or even make sense) for $x = 0$, depending on which formalism one take into account to give meaning to integrals containing δ .

$$\text{Dirac delta}(s) = \delta(s) = 1 \text{ if } s > 0, 0 \text{ if } s \leq 0$$

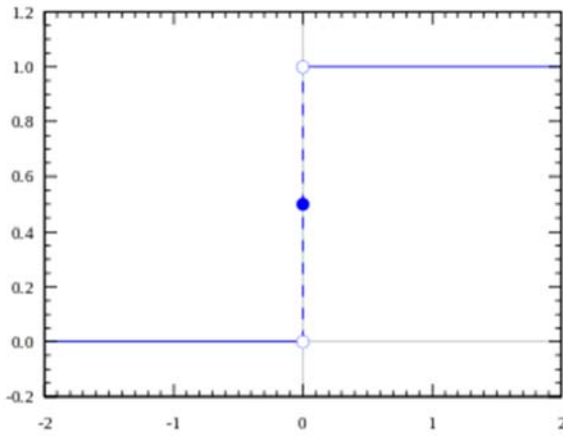


Figure 5.2: Heavisde step function (Weisstein, 2014a)

Properties of Heaviside:

1. Linearity:

$$H(ax+b) = \begin{cases} H\left(x + \frac{b}{a}\right) & a > 0 \\ H\left(-x - \frac{b}{a}\right) & a < 0 \end{cases}$$

3. Invariance property:

a. Translation

$$H(x - x_o) = H(\bullet - x_o)(x)$$

b. Scaling

$$\text{Let } a = \frac{1}{c}, c \neq 0, a > 0$$

$$H\left(\frac{x}{c}\right) = H\left(\frac{\bullet}{c}\right)(x)$$

3. Self-reversibility:

$$H(x) * H(x) = tH(t)$$

4. Fourier transform of Heaviside function

$$F_x[H(x)](k) = \int_{-\infty}^{\infty} e^{-2\pi i k x} H(x) dx$$

$$= \frac{1}{2} \left[\delta(k) - \frac{i}{\pi k} \right],$$

Where $\delta(k)$ is the delta function. The delta function is a common function that can be represented as the limit of a class of delta sequences (Weisstein, 2014a)

5. Inverse Fourier transform of Heaviside function:

$$F^{-1}(H) = \delta(K) = 1$$

We need the following Leibniz rule concept in term of Heaviside function:

Definition 5.4. By utilizing the Leibniz rule between two functions φ and f

We have

$${}_a D_t^p (\varphi(t) f(t)) = \sum_{k=0}^{\infty} \binom{p}{k} \varphi^{(k)}(t) {}_a D_t^{p-k} f(t) \quad 5.8$$

By substituting

$$f(t) = H(t - \alpha), \quad 5.9$$

where $H(t - \alpha)$ is the Heaviside order α i-e $H_\alpha(t) = H(t - \alpha)$.

$${}_a D_t^p (\varphi(t)f(t)) = \sum_{k=0}^{\infty} \binom{p}{k} \varphi^{(k)}(t) {}_a D_t^{p-k} H(t-\alpha) H(t-\alpha) \quad 5.10$$

$$= \frac{(t-\alpha)^{-p}}{\Gamma(1-p)} \varphi^{(k)}(t) {}_a D_t^{p-k} H(t-\alpha) \quad 5.11$$

$$= \frac{(t-a)^{-p}}{\Gamma(1-p)} \varphi(t) + \sum_{k=1}^{\infty} \binom{p}{k} \frac{(t-a)^{k-p}}{\Gamma(k-p+1)} \varphi^{(k)}(t) \quad 5.12$$

$$= \sum_{k=0}^{\infty} \binom{p}{k} \frac{(t-a)^{k-p}}{\Gamma(k-p+1)} \varphi^{(k)}(t) \quad 5.13$$

Where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ and $\varphi^{(k)}$ is the k orientation of the function $\varphi(t)$ and Γ

is the Euler gamma function.

5.3 Methodology

In this section two watermarking techniques are presented using FSC and HFOA.

5.3.1 Using FSC

The watermarking domain used in this technique is transform domain based on FSC. The watermark embedding and extraction is performed in FSC. Further the watermarking technique used in this study is blind watermarking technique. In blind watermarking technique original image is not required for the watermark detection and is more practical than non-blind watermarking techniques.

5.3.1.1 Watermark Embedding

For the current implementation, the watermark signal consists of $\{+1,-1\}$ bits. The watermark embedding process can be represented by the following equation:

$$S = s + (w_b \times \kappa) , \quad 5.14$$

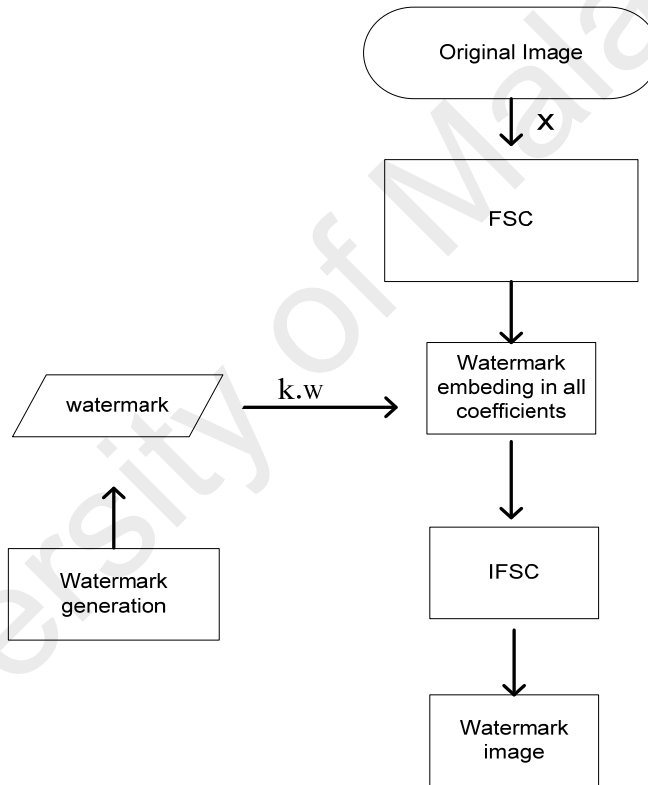


Figure 5.3: Watermark embedding scheme for the Invariant domain

where S represents the watermark signal, s is the original signal (i.e. coefficients in our case), w_b is the watermark bit. The parameter κ is a constant value.

The proposed watermarking embedding technique includes the following steps:

- i. Read the grayscale images of size 512×512.
- ii. Apply fractional Sc_α transformation:
 - a. Set the parameter $\alpha > 0$.
 - b. Fix the value of the variable t .
 - c. Calculate the fractional order of Sc_α using Definition 5.3
- iii. Embed the watermark using the equation 5.14.
- iv. Calculate inverse fractional Sc_α by taking transpose of the resultant image.
- v. Perform steps i to iv for each image.

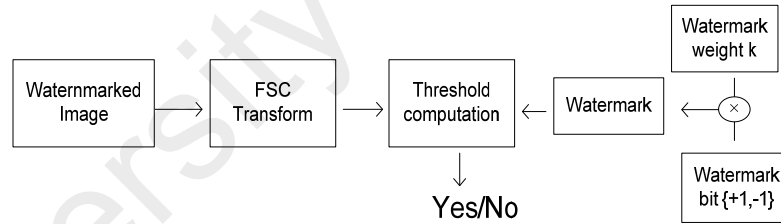


Figure 5.4: Watermark Detection.

5.3.1.2 Watermark detection

Watermark detection processes is shown in Figure 5.4. The correlation between the watermarked coefficient and the watermark to be tested for the existence is computed using the following expression:

$$\rho = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I'_0(i, j) w(i, j), \quad 5.15$$

where $I'_0(i, j)$ is the FSC coefficient and $w(i, j)$ represents the watermark. MN is the size of the image. The computed value of ρ is then compared to the threshold value T_ρ calculated as follows:

$$T_\rho = 3.97\sqrt{2\sigma_{\rho\beta}^2}, \quad 5.16$$

where $\sigma_{\rho\beta}^2$ represents the variance and

$$\sigma_{\rho\beta}^2 \approx \frac{1}{(MN)^2} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I'_0(i, j))^2 \quad 5.17$$

For the detailed derivation of these equations, we refer the interested readers to (Barni et al., 2001). The existence of the watermark will be confirmed when $\rho > T_\rho$.

The proposed technique watermark detection steps are summarize in the following pseudo code:

- i. Read the watermark/attacked image.
- ii. Apply FSC transformation on the image.
- iii. Compute ρ and T_ρ using equation 5.15 and 5.16 respectively.
- iv. Compare ρ and T_ρ , If $\rho > T_\rho$ then watermark is detected otherwise not.
- v. Repeat step i to iv for all images.

5.3.2 Using HFOA

The second function used for watermark embedding domain is HFOA.

5.3.2.1 Watermark embedding and detection

The proposed watermarking embedding technique includes the following steps:

- i. Read the grayscale images of size 512×512.
- ii. Apply fractional H_α transformation:
 - a. Set the parameter α , $0 < \alpha \leq 1$.
 - b. Fix the value of the variable t such that $t > \alpha$.
 - c. Calculate the fractional order of H_α using Definition 5.4
- iii. Embed the watermark using the equation 5.14.
- iv. Calculate inverse fractional H_α by taking transpose of the resultant image.
- v. Perform steps i to iv for each image.

5.3.2.2 Watermark detection

Watermark detection is in fact the reverse of the embedding processes. Our aim is to detect the watermark in the fractional Gaussian field (Dobrić & Ojeda, 2006). Assume the image I_α with size MN , then the covariance is given by

$$E(I_\alpha(M)I_\beta(N)) = A_{\alpha,\beta} \left(\frac{M^{\alpha+\beta} + N^{\alpha+\beta} - |M - N|^{\alpha+\beta}}{2} \right), \quad 5.18$$

where α, β are fractional numbers in (0,1) and

$$A_{\alpha,\beta} = -\frac{2}{\pi} (\sqrt{\Gamma(2\alpha+1)\sin(\alpha\pi)\Gamma(2\beta+1)\sin(\beta\pi)}) \times \Gamma(-(\alpha+\beta)) \cos((\beta-\alpha)\frac{\pi}{2}) \cos((\alpha+\beta)\frac{\pi}{2}) \quad 5.19$$

for $\alpha+\beta \neq 1$ and

Since we use the special function $\text{sinc}\alpha$, this consequently leads to change the threshold by utilizing special function such as \sin ,

$$A_{\alpha} = \sqrt{\Gamma(2\alpha+1)\Gamma(3-2\alpha)} \sin^2 (\alpha \pi) \quad 5.20$$

The fractional Gaussian field has a simple covariance structure and it is related to two generalization of fractional motion known as multifunction motions. The Gaussian field due to inherited duality reveals a new way of constructing martingales associated with the odd and even part of a fractional motion.

Assume the image I_{α} of size MN , where the M is the number of rows and N is the number of columns. Then the covariance is given by (Dobrić & Ojeda, 2006) which can be represented as follows:

$$E(I_{\alpha i}(M), I_{\beta j}(N)) = A_{\alpha, \beta} * a \quad 5.21$$

Where a can be represented as:

$$a = \left(\frac{M^{\alpha+\beta} + N^{\alpha+\beta} - |M - N|^{\alpha+\beta}}{2} \right) \quad 5.22$$

$$E(I_{\alpha i}(M), I_{\beta j}(N)) = A_{\alpha, \beta} \left(\frac{M^{\alpha+\beta} + N^{\alpha+\beta} - |M - N|^{\alpha+\beta}}{2} \right), \quad 5.23$$

Where α, β are fractional numbers. In practice the following unbiased estimate of $E(I_{\alpha i}, I_{\beta j})$ is used.

$$E(I_{\alpha i}, I_{\beta j}) \approx (I_{\alpha i}, I_{\beta j}) = A_{\alpha+\beta} \left(\frac{M^{\alpha+\beta} + N^{\alpha+\beta} - |M - N|^{\alpha+\beta}}{2} \right) \quad 5.24$$

where $A_{\alpha i + \beta j}$ can be represented by the following equation:

$$A_{\alpha i + \beta j} = -\frac{2}{\pi} \left(\sqrt{\Gamma(2\alpha + 1) \sin(\alpha\pi) \Gamma(2\beta + 1) \sin(\beta\pi)} \right) \times \Gamma(-(\alpha + \beta)) \cos\left((\beta - \alpha)\frac{\pi}{2}\right) \cos\left((\alpha + \beta)\frac{\pi}{2}\right) \quad 5.25$$

for $\alpha + \beta \neq 1$ and

$$A_{\alpha} = \sqrt{\Gamma(2\alpha + 1) \Gamma(3 - 2\alpha)} \sin^2(\alpha\pi) \quad 5.26$$

for $\alpha + \beta = 1$.

In general the variance of population of size N , is represented as:

$$\sigma^2 = \frac{1}{N} \sum_{i=1}^n (E[X])^2 \quad 5.27$$

$$\sigma^2 = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (E(I_{\alpha i}, I_{\beta j}))^2 \quad 5.28$$

In practice the following unbiased estimate of $\sigma_{\alpha\beta}^2$ is used:

$$\sigma_{\alpha\beta}^2 \approx \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [(A_{\alpha,\beta} * a) I'(i, j)]^2 \quad 5.29$$

where $I'(i, j)$ is the watermark coefficients and $(A_{\alpha,\beta} * a)$ is defined in equation

5.21. The correlation between the marked coefficients and the watermarked sequence to be tested for the presence is computed as:

$$\rho = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [(A_{\alpha,\beta} * a)I'(i, j)w(i, j)] \quad 5.30$$

We used the following threshold:

$$T_{\rho} = 3.97 \sqrt{2\sigma_{\alpha\beta}^2} \quad 5.31$$

The proposed technique watermark detection steps are summarize in the following pseudo code:

- i. Read the watermark/attacked image.
- ii. Apply HFOA transformation to the image.
- iii. Compute ρ and T_{ρ} using equation 5.30 and 5.31 respectively.
- iv. Compare ρ and T_{ρ} , If $\rho > T_{\rho}$ then watermark is detected otherwise not.
- v. Repeat step i to iv for all images.

5.4 Experimental results and discussion using FSC

In this section, we evaluate the performance of the proposed watermarking technique by considering robustness and fidelity. Five standard test images from the USC-SIPI dataset, namely, Baboon, Cameraman, Lena, Peppers, and Sailboat, are considered for evaluation purposes. These images are each of dimensions 512×512 and they are shown in Figure 5.5(a-e). The algorithm is coded by using Matlab and checkmark (Shelby Pereira, 2001) software is deployed for testing the robustness against different set of attacks. The watermark signal is presented by the sequence of +1 or -1.



Figure 5.5: (a-e) Original Test Images, (f-j) Watermarked Test Images.

5.4.1 Imperceptibility

The watermarked images obtained by using the proposed technique are shown in Figure 5.5(f-j). In each image total, 262,144 bits of watermark is embedded. By visual inspection, the watermarked images appear perceptually similar to their original counterparts. To quantify the transparency of the embedded watermark, the PSNR and SSIM are considered, which are commonly used by the watermark community. The results are recorded in Table 5.1. It is observed that the PSNR and SSIM values range from 41.37 to 42.52dB and 0.92 to 0.98, respectively. These readings suggest that the watermark image generated by the proposed method is of high perceptual quality.

Table 5.1: PSNR and SSIM value of sample test images in the proposed FSC domain.

	Lena	Baboon	Cameraman	Sailboat Boat	Peppers
PSNR	42.02	41.80	42.52	41.54	41.37
MSE	4.09	4.30	3.64	4.56	4.74
SSIM	0.93	0.98	0.92	0.95	0.94

5.4.2 Robustness

Figure 5.6(a-f) summaries the different set of attacks we performed for the evaluation of our proposed watermarking technique. Cross correlation method based on Neyman-Pearson is deployed to detect the embedded watermark and its formula is detailed in (Barni et al., 2001).

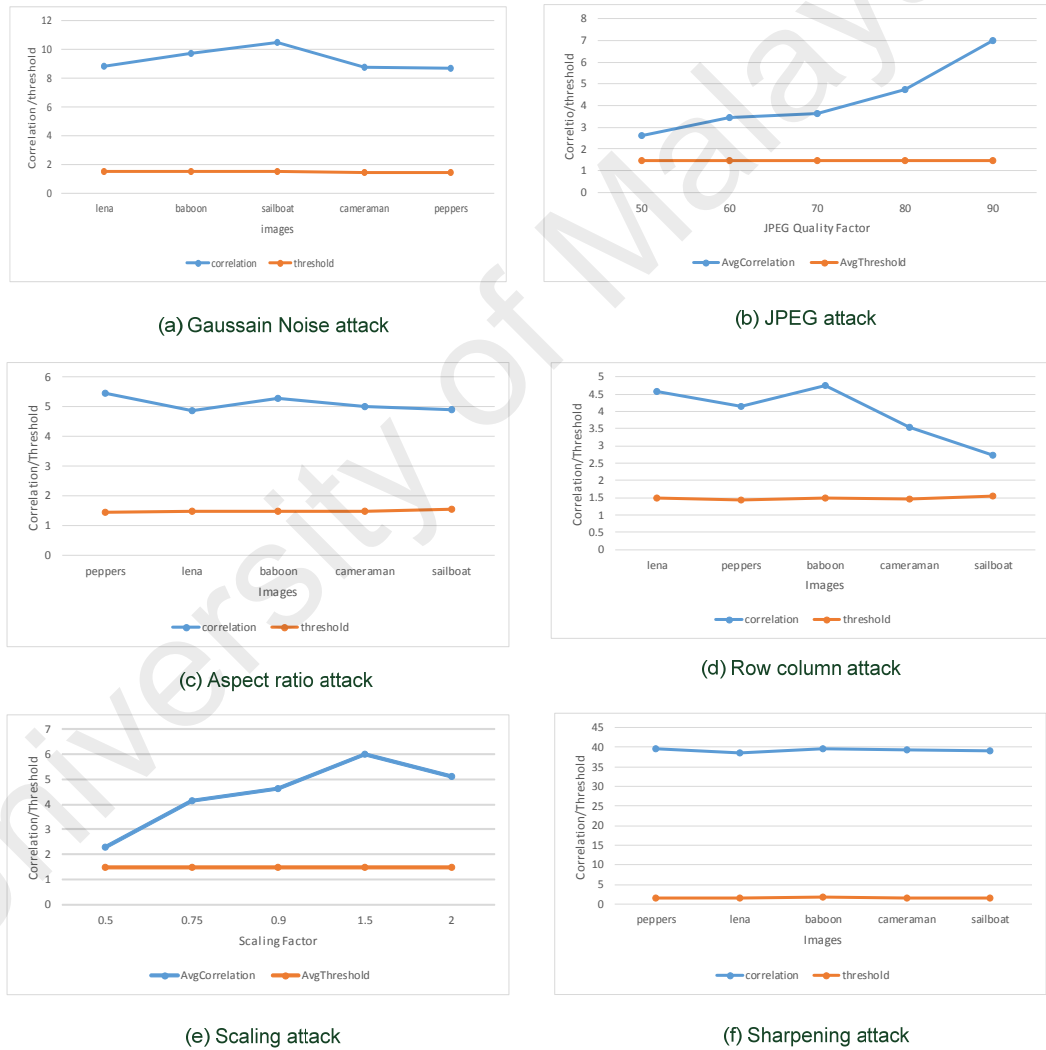


Figure 5.6: Robustness of Proposed Technique against different types of attacks. (a) Gaussian Noise. (b) JPEG Compression. (c) Aspect ratio attack. (d) Row Column removal attack. (e) Scaling attack. (f) Sharpening attack.

Here, the watermarked images have gone various types of attack to investigate the robustness of the proposed technique. In particular, each watermarked image is distorted using different geometric and image processing attacks, namely: (1) rescaling attack with scaling factor ranging from 0.5 to 2; (2) JPEG compression with quality factor ranging from 50% to 90% with increment of 10; (3) row and column removal attack with the number of rows and column removal varying from 1 to 17; (4) change in aspect ratio in the x and y directions; (5) Gaussian filtering with kernel size of 3×3 and 4×4 pixels; (6) sharpening attack. (7) Cropping attack with 10, 20 and 50% cropped relative to the size of image; Figure 5.7(a- t) shows the result of applying these attacks.

Next, we evaluated the performance of the proposed under different attacks and the results are summarized in Figure 5.6(a-b) and Figure 5.8(a-b). The cross correlation computation based on Neyman-Pearson criterion and the threshold value are considered to test the presence of the embedded watermark.

The scaling attack using various factors ranging from 0.5 to 2.0, ρ remains well above the (i.e., threshold) considered as suggested by Figure 5.6(e). Robustness against JPEG compression with quality factor ranging from 50% to 90% are shown in Figure 5.6(b). The presence of watermark is detected in all these cases, as the Correlation values lies quite above the threshold value. moreover, common image processing operations such as, aspect ratio change Figure 5.6(c), row and column removal attack Figure 5.6(d), sharpening and Gaussian filtering Figure 5.6(a,f) are also applied on the watermarked image. For all cases, the dynamically computed ρ value always stays above the threshold, i.e., 100% successful detection. Therefore, the results suggest that the proposed method is robust against the commonly considered watermarking distortion attacks.

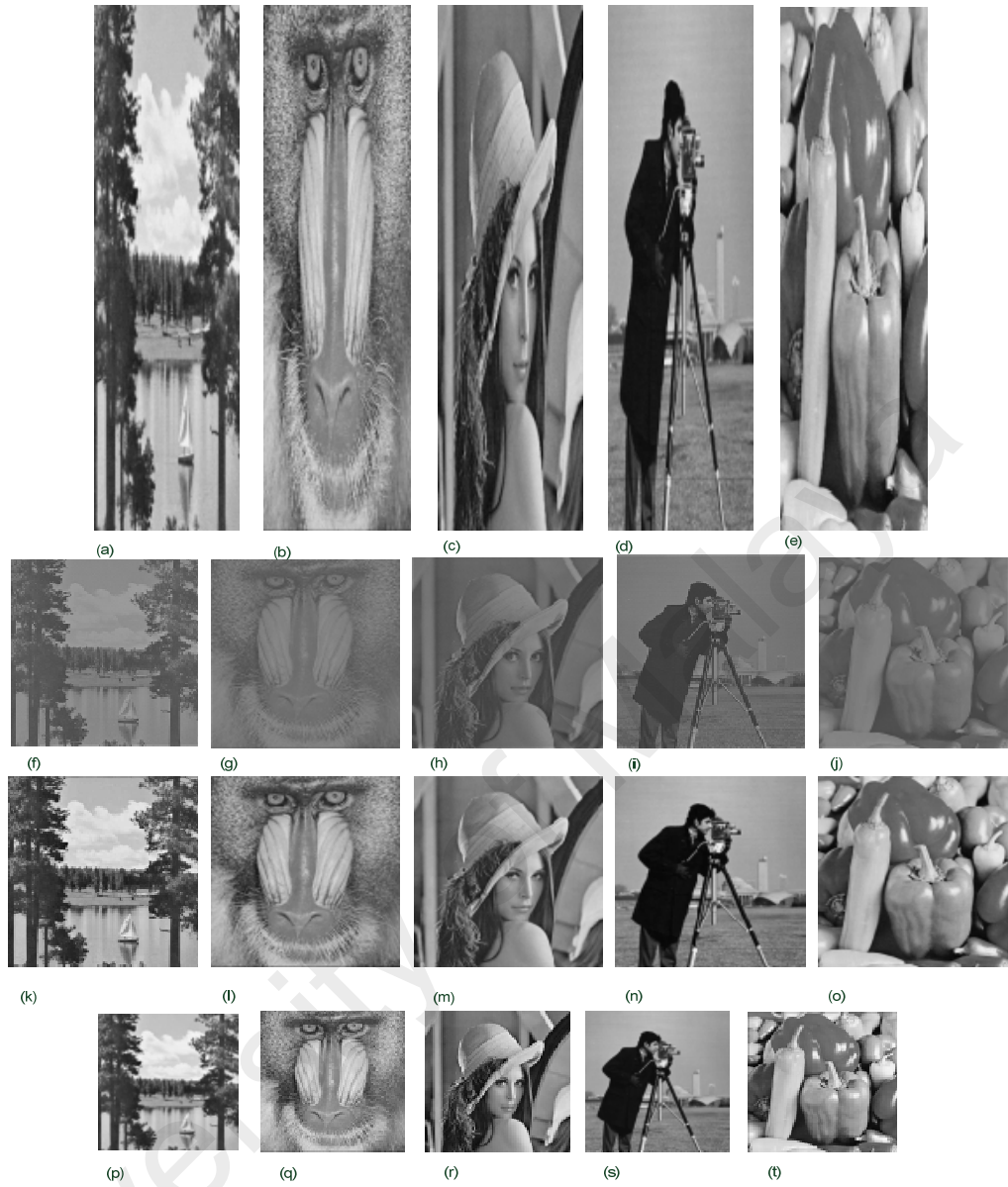


Figure 5.7: Experimental results:(a) to (e) show the watermarked test images manipulated by using aspect ratio of 2:7 in relation to x and y axis; (f) to (j) represent watermarked images corrupted by using sharpening attack;(k) to (o) illustrate the watermarked images are compressed with JPEG compression attack with quality factor 50;(p) to (t) display the scaled down to 50% of the image size.

With the aforementioned observations, we conclude that the proposed method performs better than the conventional watermarking method.

5.5 Fractional Rotation matrix expression

We derived a new method to achieve the rotation invariance using fractional trigonometric functions. Now let us examine rotation of images by utilizing method based on the fractional derivative D^α of $\sin(t)$ and $\cos(t)$. We have the following result

Lemma 5.1 Let $\cos(t)$ and $\sin(t)$ defined respectively by

$$\cos_\alpha(t) = \sum_{n=0}^{\infty} \frac{t^{n-\alpha}}{\Gamma(n-\alpha+1)} \cos\left((n-\alpha)\frac{\pi}{2}\right) \quad 5.32$$

And

$$\sin_\alpha(t) = \sum_{n=0}^{\infty} \frac{t^{n-\alpha}}{\Gamma(n-\alpha+1)} \sin\left((n-\alpha)\frac{\pi}{2}\right). \quad 5.33$$

Then we have the fractional rotation

$$R_\alpha = \begin{pmatrix} \cos(\alpha\pi/2) & \sin(\alpha\pi/2) \\ -\sin(\alpha\pi/2) & \cos(\alpha\pi/2) \end{pmatrix}.$$

Proof. By using Definition 5.2 together with Remark 5.1, we obtain that

$$D^\alpha \sin(t) = \sin(\alpha\pi/2) \cos_\alpha(t) + \cos(\alpha\pi/2) \sin_\alpha(t) \quad 5.34$$

and

$$D^\alpha \cos(t) = \cos(\alpha\pi/2) \cos_\alpha(t) - \sin(\alpha\pi/2) \sin_\alpha(t) \quad 5.35$$

A geometrical interpretation of the derivative relations in equation 5.34 and equation 5.35 can be found by imposing the matrix form

$$R_{D^\alpha} = \begin{pmatrix} D^\alpha \cos(t) & D^\alpha \sin(t) \end{pmatrix}. \quad 5.36$$

Collecting the coefficients of R_{D^α} , we receive the following fractional rotation matrix:

$$R_{\alpha} = \begin{pmatrix} \cos(\alpha\pi/2) & \sin(\alpha\pi/2) \\ -\sin(\alpha\pi/2) & \cos(\alpha\pi/2) \end{pmatrix} \quad 5.37$$

By applying rotation using equation 5.36 of different degrees such as 5, 10, 15, 20, 25, 30, 35, 40 to the images we get fractional rotation.



Figure 5.8 (a-d) Rotation achieved using fractional rotation expression having angle 15, 25, 30 and 45 respectively.

Remark 5.2 One can use the transpose of $R_{D^{\alpha}}$ to get good result as well.

$$R_{\alpha}^T = \begin{pmatrix} \cos(\alpha\pi/2) & -\sin(\alpha\pi/2) \\ \sin(\alpha\pi/2) & \cos(\alpha\pi/2) \end{pmatrix}.$$

5.6 Experiments results and discussion using HFOA

After discussing the experiments using FSC as watermark domain, now we discuss experimental results using HFOA as watermark domain.

5.6.1 Imperceptibility

The watermarked images obtained by using the proposed technique whereas total 262,144 bits of watermark is embedded in each image. To quantify the transparency of the embedded watermark, PSNR and SSIM are considered, which are commonly used by the watermark community. The results are recorded in Table 5.2. It is observed that the PSNR and SSIM values range from 37 to 38 dB and 0.88 to 0.94, respectively. These

readings suggest that the watermark image generated by the proposed method is of good perceptual quality.

Table 5.2: PSNR and SSIM value of sample test images in the proposed HFOA domain.

Images	Lena	Baboon	Cameraman	Sailboat Boat	Peppers
PSNR	38	37	38	37	37
MSE	11	12	10	13	13
SSIM	0.88	0.94	0.92	0.95	0.94

5.6.2 Robustness

The watermarked images have undergone various types of attack to investigate the robustness of the proposed technique. In particular, each watermarked image is distorted using different geometric and image processing attacks, namely: (1) scaling attack with scaling factor ranging from 0.5 to 2; (2) JPEG compression with quality factor ranging from 50% to 90% with increment of 10; (3) row and column removal attack with the number of rows and column removal varying from 1 to 17; (4) change in aspect ratio in the x and y directions; (5) Gaussian filtering with kernel size of 3×3 and 4×4 pixels; (6) sharpening attack. (7) Cropping attack with 10, 20 and 50% cropped relative to the size of image; (8) Rotation attack with cropping option, having rotation angle from -2 to 45 degrees; (9) Random bending attack with wrap factor value changes from 2 to 4; (10) Circular shift attack 50% of image size.

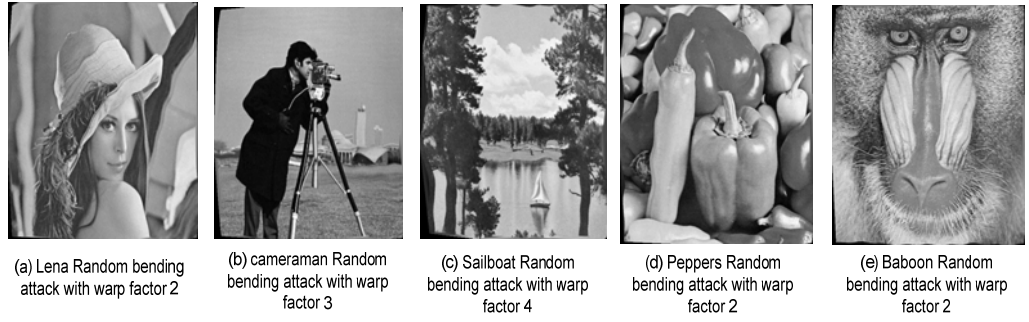


Figure 5.9: (a-e) Watermark test images: Random bending attack with wrap factor value changes from 2 to 4



Figure 5.10: (a-e) Original Test Images, (f-j) Attacked watermarked Test Images: Rotation attack for different values of the angels are taken as 5,10,15,30 and 45 respectively.

Robustness against JPEG compression with quality factor ranging from 50% to 90% are successfully tested. The presence of watermark is detected in all these cases, as the Correlation values lies quite above the threshold value. Moreover, common image processing operations such as, aspect ratio change , sharpening attack and random bending attack Figure 5.9(a-e) are also applied on the watermarked image. For all cases, the dynamically computed ρ value always stays above the threshold, i.e., 100% successful detection.

Next, we evaluate the performance of the proposed technique under different attacks and the results are summarized in Figure 5.11(a-f), Figure 5.12. The cross correlation computation based on fractional Gaussian field criterion and the threshold value are considered to test the presence of the embedded watermark.

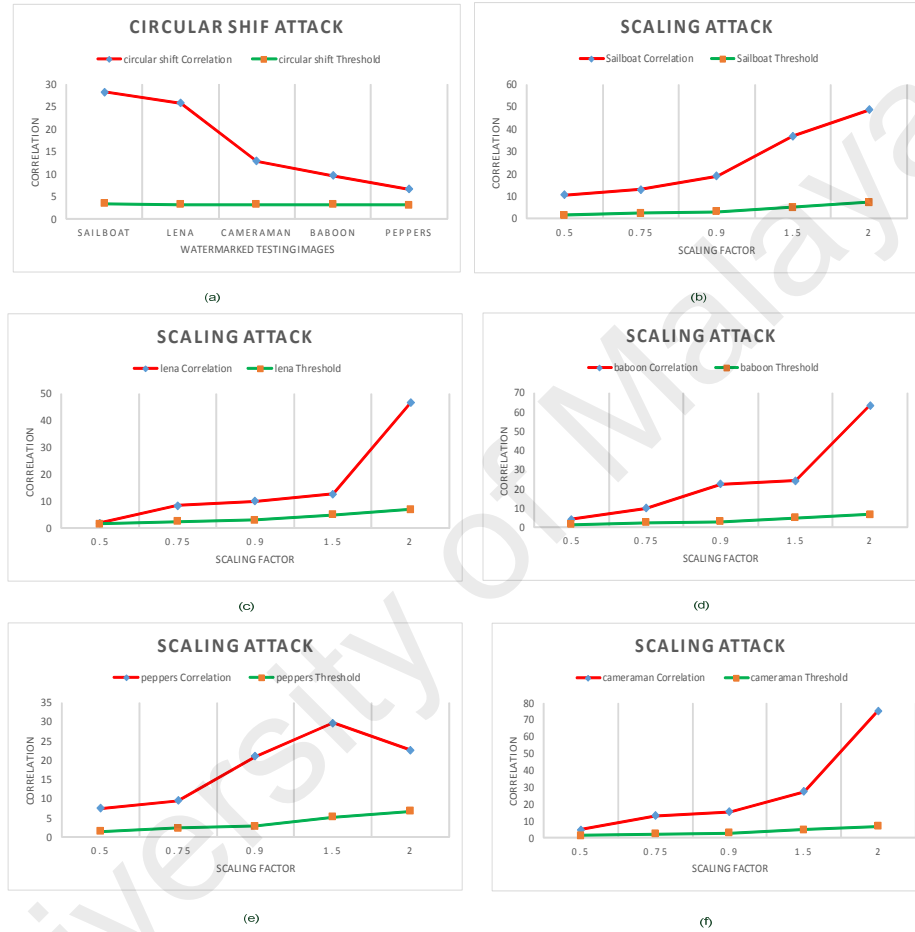


Figure 5.11: Robustness against scaling and circular shift Attack: (a) Comparison of the Correlation and Threshold values of five watermarked test images against the circular shift attack. (b-f) Comparison of Correlation values of five images after scaling attack of the proposed technique.

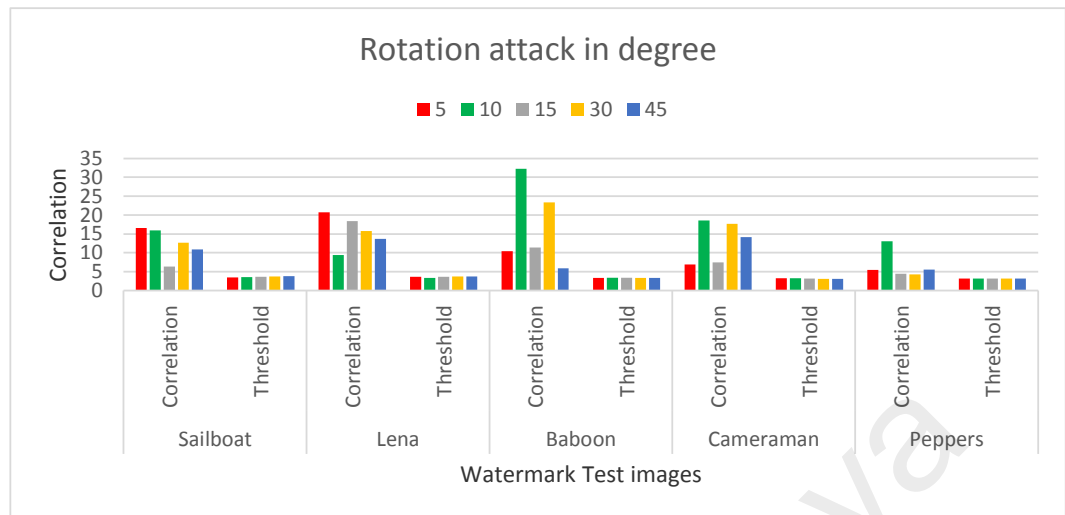


Figure 5.12: Robustness of Proposed Technique against Rotation attacks. Five standard images are tested for the rotation attack. Rotation angle is taken of different values such as 5, 10, 15, 30, 45 degrees.

Robustness against RST attack has been tested successfully. Figure 5.11(a) represent the correlation value of five watermark images after the circular shift attack. The circular shift operation is set as the 50% of the image size. The correlation value of the attack image remains above the threshold value which confirm that the proposed technique is robust against the circular shift attack. Figure 5.11(b-f) represent the correlation values of five watermark images after scaling attack using scaling factors ranging from 0.5 to 2.0, ρ remains well above the (i.e., threshold). Therefore, the results suggest that the proposed method is robust against the scaling attack. Last but not the least Figure 5.12 represent the comparison of correlation value against the threshold value, after the rotation attack. The result confirm that the proposed technique is robust against the rotation attack.

The result shows high level of robustness of our proposed technique as watermark has been detected in all the images.

5.7 Chapter Summary

Digital image watermarking is an important technique for the multimedia content authentication and copyright protection. Some watermarking techniques are extremely robust but they suffer poor imperceptibility. We introduce a watermarking algorithm balanced between fidelity and robustness based on fractional calculus. We have constructed a domain using FSC. The FSC model the signal as a fractional polynomial for watermark embedding. Watermark is embedded in all the coefficients of the image. Cross correlation method based on Neyman-Pearson is used for watermark detection. Experimental results confirmed the proposed technique is robust and imperceptible. Improvement of PSNR value of watermark images are almost double. Common test for robustness shows watermark can be detected after most of the attacks.

We also introduce invariant watermarking algorithm based on HFOA. The advantage of RST invariant domain is the elimination of resynchronization during watermark detection. We have constructed a domain using HFOA. We have also constructed cross correlation method based on fractional Gaussian field for watermark detection. Experimental results confirmed the proposed technique is highly robust especially to RST attacks.

CHAPTER 6: FUZZY LOGIC AND WAVELET TRANSFORM BASED WATERMARKING FOR 3D IMAGES

With the advancement in the processing capabilities of computers, the use of three dimensional objects (3DObjects) in different fields has been increased in recent years. Moreover the cost of 3D display devices has also become cheaper. A brief introduction of DIBR 3D images was presented in the chapter 2. DIBR of a 3D image is a 3D image representation consisting of center image and depth image.

6.1 Initial study of wavelet based watermarking for 3D Images

In this section a watermarking scheme is presented (Almas Abbasi, 2013) for the protection of center image contents using the depth values of the 3D objects, of the depth image. We design IT2FLS based HVS model, to perform watermark embedding, in an image using image features such as contrast sensitivity, luminance and entropy in wavelet domain. We used HL, LH sub-band at second level of 2D-DWT for watermark embedding. The watermark is usually embedded in middle frequency part of the image. As changes made to low frequency part i-e., LL sub-band can easily be visible to human eye, while the high frequency part i-e., HH sub-band is more sensitive to compression and scaling operation. That's why HL, LH sub-band is used for watermark embedding.

IT2FLS is used to, intelligently determine masking value, for each coefficient of the Image in Discrete Wavelet Domain to embed watermark imperceptibly using HVS model. We designed 45 rules to take into account all the possible combination of the three inputs to produce watermark masking weight factor, for each of the selected DWT coefficient. These three inputs are entropy, contrast and luminance masking. The depth values of the coefficients are used as selection criteria for watermark embedding. For watermark

embedding only those coefficients are selected in Morton order which have depth value greater than empirically determined threshold value.

Keeping in view the limitation of human perceptual ability to depth, we also tried to exploit the depth value of the image pixels for watermark embedding. The PSNR, MSE and BER (Bit Error Rate) values of watermarked center images for each of the tested images are listed in Table 6.1. The size of the images are 1390×1110 pixels. The experimental results show that the proposed technique embed watermark with least distortion and it is robust to JPEG compression and Noise attack of different variance as shown in Tables 6.2 and 6.3.

Table 6.1: PSNR, MSE and BER values of watermarked center testing images.

Images	Books	Art	Doll	Moebius
PSNR	57.3067	53.5209	53.7633	53.3406
MSE	0.1209	0.2891	0.2734	0.3013
BER	0.5159	0.4951	0.5012	0.5113

Table 6.2: PSNR, MSE and BER values of Watermark Center Image after applying Gaussian Noise Attack of Different Variance Such As 50, 100, 150, 200.

Attacks		Doll	Art	Books	Moebius
Gaussian Noise 50 variance	<i>PSNR</i>	33.7919	33.5344	37.2546	33.5765
	<i>MSE</i>	27.1577	28.8163	12.2353	28.5387
	<i>BER</i>	0.5095	0.5010	0.5000	0.5181
Gaussian Noise 100 variance	<i>PSNR</i>	32.1316	31.8824	35.5876	31.9157
	<i>MSE</i>	39.8031	42.1544	17.9604	41.8325
	<i>BER</i>	0.5085	0.4959	0.4999	0.5150
Gaussian Noise 150 variance	<i>PSNR</i>	31.4141	31.1656	34.8614	31.1994
	<i>MSE</i>	46.9543	49.7192	21.2293	49.3340
	<i>BER</i>	0.5078	0.5034	0.4990	0.5142
Gaussian Noise 200 variance	<i>PSNR</i>	30.9915	30.7552	34.4207	30.7784
	<i>MSE</i>	51.7520	54.6460	23.4968	54.3552
	<i>BER</i>	0.5084	0.5032	0.4985	0.5147

Table 6.3: PSNR, MSE and BER values of Watermark Center Image after Applying JPEG Compression Attack of Different Quality Factors such as 50, 60, 70, 80, 90, 100.

Attacks		Doll	Art	Books	Moebius
Jpeg50	<i>PSNR</i>	42.57	39.83	46.35	42.84
	<i>MSE</i>	3.6	6.77	1.51	3.38
	<i>BER</i>	0.5208	0.5416	0.5413	0.5454
Jpeg60	<i>PSNR</i>	43.66	40.69	47.6946	43.9071
	<i>MSE</i>	2.80	5.5470	1.1057	2.6447
	<i>BER</i>	0.5197	0.5437	0.5535	0.5084
Jpeg70	<i>PSNR</i>	45.01	40.3286	49.0526	45.2974
	<i>MSE</i>	2.05	6.0286	0.8088	1.9202
	<i>BER</i>	0.4986	0.5290	0.5125	0.5183
Jpeg80	<i>PSNR</i>	46.72	43.1347	50.7150	46.9595
	<i>MSE</i>	1.3826	3.1594	0.5515	1.3096
	<i>BER</i>	0.5108	0.5232	0.5284	0.5248
Jpeg90	<i>PSNR</i>	48.73	45.2067	52.8446	48.7511
	<i>MSE</i>	0.87	1.9607	0.3378	0.8669
	<i>BER</i>	0.496	0.4970	0.5209	0.5053
Jpeg100	<i>PSNR</i>	50.30	48.9596	54.4361	49.9879
	<i>MSE</i>	0.61	0.8263	0.2341	0.6521
	<i>BER</i>	0.5010	0.5009	0.5214	0.5100

6.2 Multidimensional wavelet based watermarking for depth image based rendering 3D images

With the advancement in the processing capabilities of computers, the use of three dimensional objects (3D Objects) in different field has been increased in recent years. Moreover the cost of 3D display devices has also become cheaper. Brief introduction of DIBR 3D images has presented in the chapter 2. DIBR of a 3D image is a 3D image representation consisting center image and depth image. In this chapter a watermarking scheme is proposed in Multi-dimensional wavelet transformation (MDWT) to protect the 3D data of DIBR 3D images.

We focused on the robustness and imperceptible capability of the watermark in the proposed algorithm. We have implemented the technique in MDWT. MDWT has proved to be a robust domain to geometrical attack (J. Li, Bai, Du, & Chen, 2011) that's why we prefer this domain for the 3D DIBR scenario.

Further with the intention to accomplish better results that of, watermark imperceptibility along with robustness, we developed IT2FLS based model to improve watermark embedding strength, while keeping the imperceptibility requirement. We calculated NVF and entropy of the selected coefficients to embed the watermark imperceptibly. The watermark is embedded in the center image and is detected in the right image after rendering operation. The results are compared with (Y.-H. Lin & Wu, 2011).

The experimental results show that the proposed technique is robust as well as imperceptible as watermark is retained in the rendered left and right images. Moreover, the BER of the extracted watermark is nearly negligible. The proposed technique embed watermark with least distortion and it is robust to JPEG compression, depth image alteration, Gaussian noise and rotation attacks.

6.3 Methodology

Our proposed technique works in a scenario. We suppose that depth image, which indicate the depth values of objects and the center image a 2D image, are passed through the communication channel. After passing through communication channel, left and right images are generated, through rendering process. In this scenario watermarking technique is proposed for a 3D DIBR system. In DIBR 3D Image system only center image C_{img} and depth image D_{img} are transmitted to the consumer side. The C_{img} is wrapped pixel wise to generate right and left eye image using the depth value from the D_{img} . The depth values are mapped between 0 to 255 represented by Z_{far} , Z_{near} as farthest and nearest clipping plane respectively.

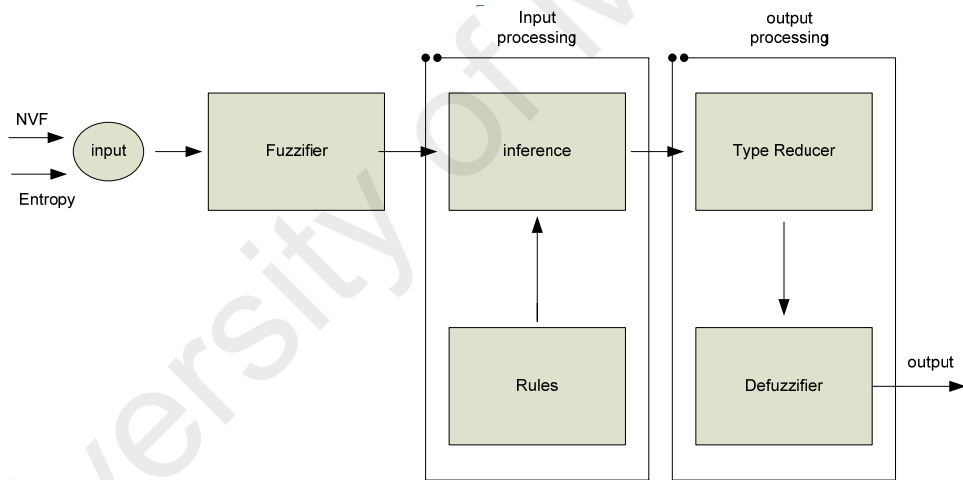


Figure 6.1: Overview of IT2FLS inputs and output for the proposed scheme.

We test the robustness of our proposed technique against geometrical attacks specially rendering. Let L_{img} , and R_{img} represent the left eye and right eye image respectively and $B_{pth,l}$ and $B_{pth,r}$ represent the pth block in the L_{img} and R_{img} . When rendering operation is applied on C_{img} to generate L_{img} and R_{img} , we can estimate the rendered block $B_{pth,l}^r$, $B_{pth,r}^r$ which represent the corresponding pixels in the the C_{img} image for the left image L_{img} and the right image R_{img} .

According to (Zhang & Tam, 2005) the rendering operations warps the pixel location according to the depth value using the following equations:

$$x_l = x_c + \frac{tx}{2} \frac{f}{z} \quad (6.1)$$

$$x_r = x_c - \frac{tx}{2} \frac{f}{z} \quad (6.2)$$

where x_l , x_r , x_c represent the corresponding pixels, in x-coordinate for the left eye image, right eye image and centre image respectively. f is the focal length of camera, tx is the baseline distance. The z represents the depth value of the pixel.

6.3.1 Watermark embedding and detection

Figure 6.2 shows our proposed protecting scheme for the center image. The center image is divided into M blocks of size N . 1st level of multidimensional discrete wavelet transform for the x direction is calculated for each block and watermark is embedded into 28 coefficients in CA sub-band using Morton order. According to (J. Li et al., 2011) low frequency coefficients (CA) are quite robust to geometric attacks. The coefficient magnitudes may change when scaling, rotation, translation and cropping attack are applied, but signs of the low frequency coefficients remain unaffected. That's why we choose CA sub-band for watermark embedding. The strength of watermark α for each coefficient is calculated through the IT2FLS. α can be represented by the following equation:

$$\alpha(i, j) = f(nvf(i, j), e(i, j)) \quad (6.3)$$

where nvf the noise visibility is function value and e is the entropy of image coefficients. nvf and e values are calculated for those coefficients selected for the watermark embedding and these are the inputs to IT2FLS. We developed 25 rules to take into account all possible combination of inputs to produce watermarking masking weight factor for the selected coefficients. The rules are in the form of

If (Condition1) and (Condition2) and (Condition3) then action.

Where the action is the output calculated by IT2FLS based on the values of two inputs.

The fuzzy rules are derived based on the following facts:

- a. Noise is more visible in flat area compared to texture region.
- b. Higher the texture, greater the ability to hide noise.

The output from the IT2FLS is the weight value calculated by IT2FLS intelligently for the selected coefficient such that when this weight factor is multiplied with the watermark and embedded in the coefficient it is least visible, fulfilling the imperceptibility condition of watermarking. Watermark consists of $\{+1, -1\}$ sequence. Watermark embedding in our technique can be represented by the following equation:

$$S = s + (w_b \times \alpha)w_p \quad (6.4)$$

where S represent watermark signal, s the original signal i.e. multidimensional wavelet coefficients in x direction, w_b the watermark bit, w_p is the reference pattern.

The watermark detection procedure is carried out by taking normalized inner product of watermark coefficient and reference pattern. This can be represented as follows (Y.-H. Lin & Wu, 2011).

$$\eta = \frac{S + w_b, w_p}{\sigma^2 w_p} \quad (6.5)$$

The sign of η is used to determine the estimated bit b'' . The BER of extracting message M from a given image I , by using the reference pattern w_p , is denoted as

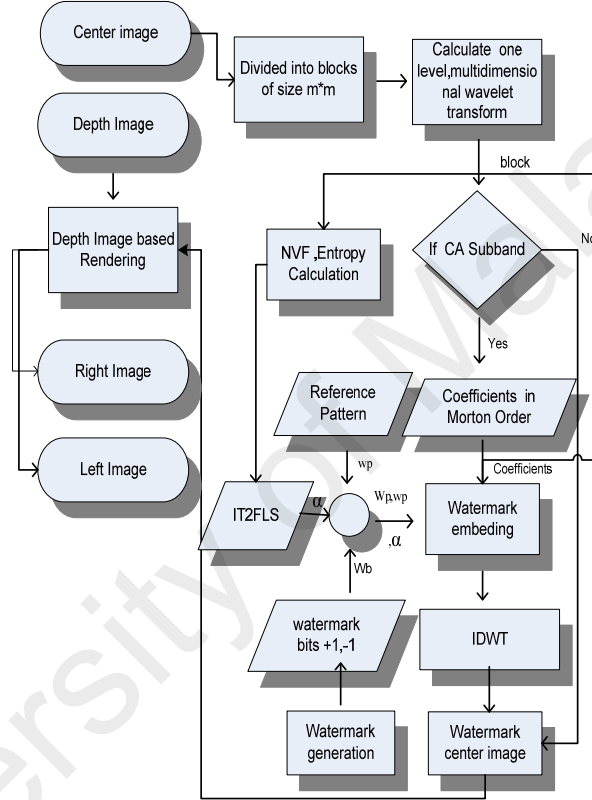


Figure 6.2: Proposed watermarking Embedding Scheme.

$$BER(I, w_p) = \frac{\text{number of } (b''_i \text{ in } M \neq b_i \text{ in } M)}{N} \quad (6.6)$$

where the N is the total number of bits of a message.

6.3.2 Hole filling

When rendering operation is performed in the DIBR 3D images, the left and right image are generated. These images contain holes due to sharp change in the depth value of the resultant images after rendering. These holes actually represent some of the objects which are occluded in the centre image but are revealed in the rendered left and right images. To reduce the complexity of the algorithm i-e polar interpolation we use linear interpolation algorithm for the hole filling predicament. In our technique we did not take into account those blocks, which contain more than 10% of holes of their size in watermark detection step.

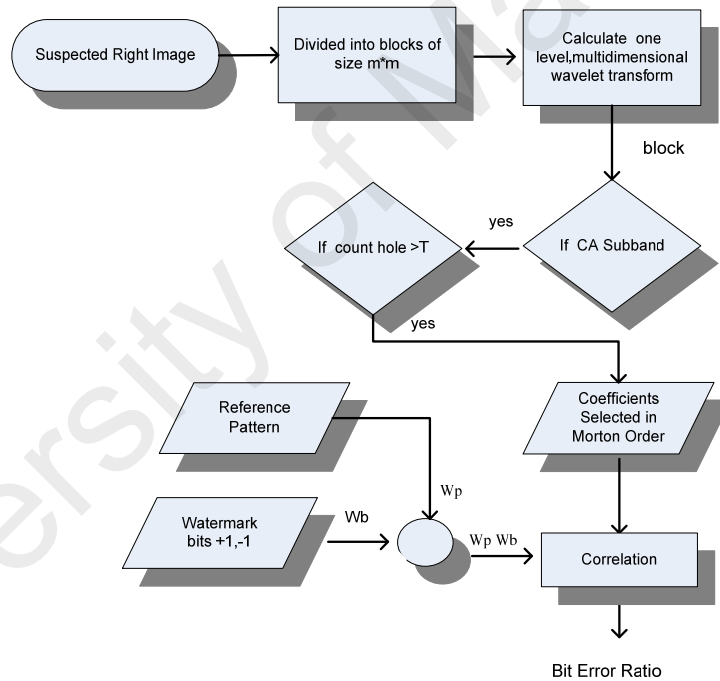


Figure 6.3: Watermark detection in the proposed scheme.



Figure 6.4: 3D original center images and depth images.

6.4 Experimental Results and Discussion

We applied our proposed technique on the images shown in Figure 6.4. The sizes of center and depth images are 1390×1110 pixels. Image sizes are reset to the nearest multiple of block 8×8 image size. We exploit the entropy masking effect to calculate the watermark weight factor. We calculated entropy of the selected image coefficient and IT2FLS determine the appropriate watermark weight factor to embed the watermark imperceptibly in these selected coefficients. Higher the entropy values of the image coefficient higher its ability to hide the watermark imperceptibly.

Table 6.4: PSNR, MSE values of Watermarked center image show the watermark detection in the rendered right image with calculated BER.

Center Images	PSNR	MSE	BER
Art	51.0134	0.5149	0.00035236
Books	54.8199	0.2143	0.00021367
Doll	51.2858	0.4836	0.00038676
Interview	52.5186	0.3641	0.00051376
Moebius	50.8838	0.5305	0.00017177

Depth image is gray scale image. The focal length and baseline distance t_x are set to 1 and 36 pixels respectively. The size of the block is set to 8×8 pixels. The length of reference pattern w_p is set 28. Watermark bits are embedded into 28 coefficients per block in Morton order.

6.4.1 JPEG Compression attack

The BER decrease significantly when we embed reference pattern in MDWT domain as indicated in Table 6.4. Figure 6.5, demonstrates the PSNR values for the JPEG compression attack for the different quality factors such as 50, 60, 70, 80, 90 and 100. For the quality factor 50 the BER approaches to 0%. Figure 6.5(b) to 6.5(d) represent the PSNR value of the rendered right eye image. These rendering is performed using the JPEG compressed centre image. JPEG attack with different quality factor is applied on the centre image. The PSNR value reaches to 46 with quality factor 50.

Figure. 6.5(c) illustrates PSNR value reaches 42 for the JPEG attack with a quality factor 10. The proposed watermarking scheme is relatively robust as it can stand high alteration in the depth image in which variance of the added Gaussian noise can reach 20000. The BER for the rest of the data is approaches to 0%. Figure. 6.5(c) implies that the proposed scheme is robust to alteration of the depth image attack.

6.4.2 Gaussian Noise Addition attack

For zero mean Gaussian noise attack with variance 50, 100, 150 and 200 the PSNR values for the centre images are shown in Figure. 6.5. When we add a zero mean Gaussian noise of variance 200 the BER is approaches to 0%. This implies that our proposed technique is robust to this class of attack.

Figure. 6.5(b) represent experimental result for adding Gaussian noise of variance zero mean with different value of variance. The PSNR value is about 34 by adding Gaussian noise of variance 200. The deformation induced due to Gaussian noise addition is visible.

6.4.3 Rotation attack

Fig 6.6(a) and 6.6(b) show that the watermarked center image is rotated clockwise by 20 and 40 degree respectively. PSNR value of the rendered right image based on rotated center image is 28.5 dB and BER 0.0017% for the 40 degree rotation and 28 dB and BER 0.0015% for the 20 degree rotation. BER for applying rotation of different degree such 5, 10, 15, 20, 25, 30, 35, 40 to the proposed scheme approaches to zero. This is because low frequency coefficients (CA) are quite robust to geometric attacks. The coefficient magnitudes may change when scaling, rotation, translation and cropping attack are applied, but signs of the low frequency coefficients remain unaffected (J. Li et al., 2011). Therefore it can be concluded that our proposed technique is robust against the rotation attacks.

Through compression and Gaussian Noise attack. The rendering operation will be based on the effected depth image. The JPEG compression and Gaussian noise addition to the depth image and its usefulness on our proposed technique is also explored.

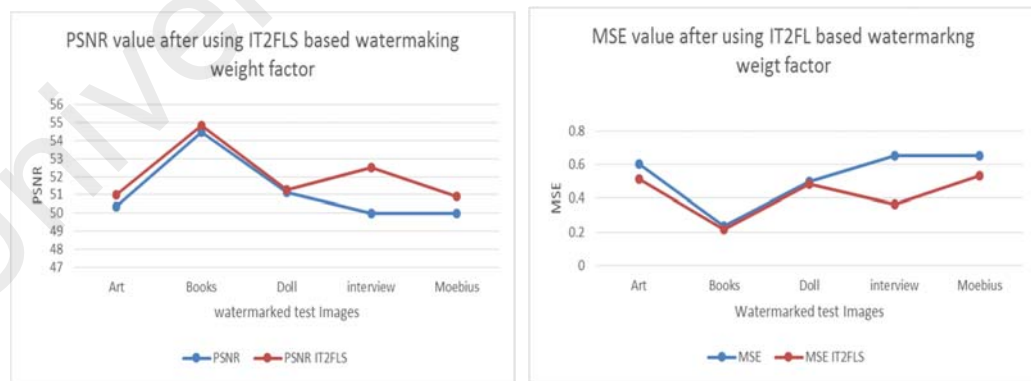


Figure 6.5(a). Comparison of PSNR and MSE values of five standard watermarked images using constant weight factor and the weight factor determined using IT2FLS respectively.

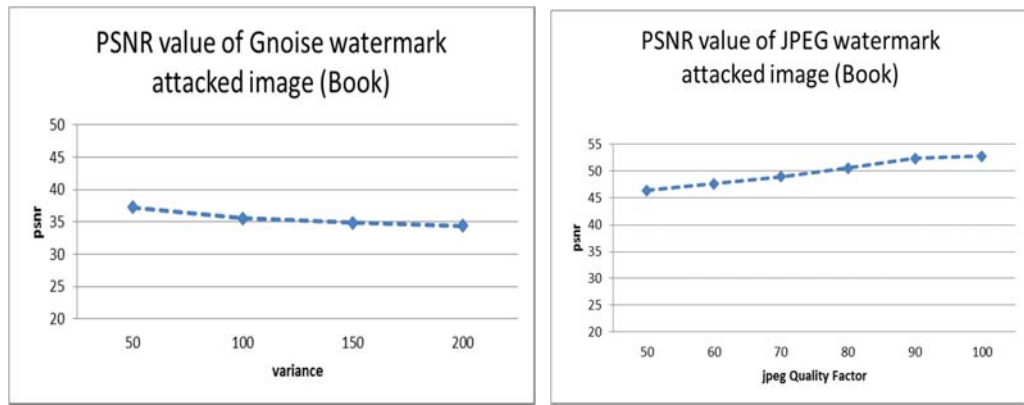


Figure 6.5(b). Comparison of PSNR values of watermarked Book images after the Gaussian Noise and JPEG compression attack respectively.

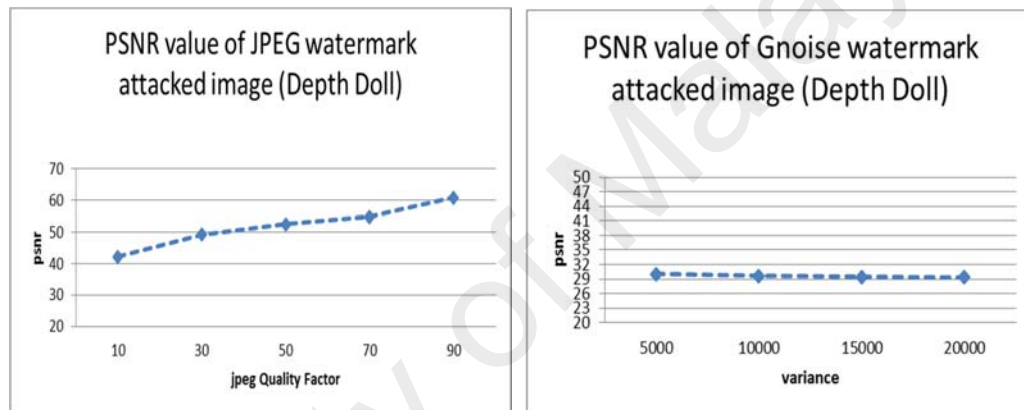


Figure 6.5(c): Comparison of PSNR values of watermarked depth image of Doll after the JPEG compression and Gaussian Noise addition attack.

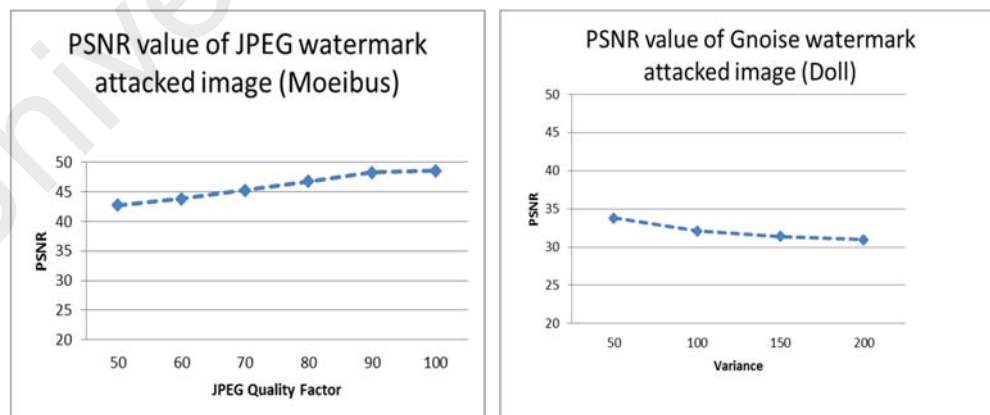


Figure 6.5(d). Comparison of PSNR values of watermarked Moeibus and Doll images after the JPEG compression and Gaussian Noise addition attack respectively.



Figure 6.6: Rotation and Gaussian noise attack effect on different 3D watermarked center images.

6.4.4 Comparison with existing technique

We compared our technique in term of imperceptibility and robustness with similar work (Y.-H. Lin & Wu, 2011). To quantify the transparency of the embedded watermark, the PSNR considered, which are commonly used by the watermarked community. The results are recorded in Table 6.4. It is observed that the PSNR values of our technique range from 50.8838 to 54.8199dB while Lin et al., has 39.40 to 43.75. This show our proposed technique has good level of imperceptibility. It is due to the use of wavelet domain and the weight factor calculated using IT2FLS based on entropy and noise visibility function. For JPEG compression attack, Gaussian noise addition attack and rotation attacks, our technique achieved BER value approaches to 0 while for (Y.-H. Lin & Wu, 2011), BER reaches to 50% for JPEG compression with quality factor 50, about 40% for Gaussian noise attack and above 40% for the geometric attack.

With the aforementioned observations, we conclude that the proposed method performs better than the conventional watermarking method considered.

6.5 Chapter Summary

In this chapter an imperceptible and robust watermarking scheme is proposed in MDWT domain for the content protection of DIBR, an image representation for 3D data. The watermark is embedded in the center image and after warping, the watermark can still be extracted in the right and left eye image. Moreover resultant BER of the extracted watermark is decreased to zero value. This shows that the proposed scheme is robust to the rendering operation. IT2FLS is used to intelligently determine weight factor for the coefficients selected for the watermark embedding, using noise visibility and entropy value. The entropy characterizes the texture of the input image. Higher the entropy values of the image coefficient higher its ability to hide the watermark imperceptibly. We use entropy to determine the texture level of image coefficient and used it for creating mask to hide the watermark more efficiently. This weight factor is used to embed the watermark imperceptibly. The experimental results illustrate that the proposed technique is robust as well as imperceptible to JPEG compression and zero mean Gaussian noise addition attack as the BER of the extracted watermark is nearly negligible. Moreover imperceptibility and robustness of the proposed scheme is checked for the rotation attack and depth image variation. The experimental results prove that the proposed technique is quite tolerant to these kinds of attacks.

CHAPTER 7: CONCLUSIONS

Digital watermarking techniques has been used to deal with issues like copyright protection and authentication to protect legitimate right of the owner and prevent illicit attempt to supersede it by the adversaries. These issues have become a matter of concern due to pervasive usage of digital media at various platforms in recent years. There is a need of developing a truly robust watermark domain to handle complicated and complex attacks. Additionally, new invariant watermarking domain should be constructed to find optimal solution for these issues. Robust watermarking techniques are usually applied for copyright protection, content authentication and temper localization because it can resist various kinds of manipulations on it.

The aim of this research mainly focuses on the two important watermarking properties. These are robustness and imperceptibility of watermark in 2D and 3D DIBR images. We investigated the limitations of the current watermarking domains. We realized that robustness, especially against RST attack is a challenging task. Moreover, truly invariant domain and 3D DIBR image watermarking has not been extensively explored. We proposed three different schemes to overcome the limitations. We evaluated the new schemes for copyright protection and temper detection. We have designed and experimented to achieve the aim and objectives in order to answers the research questions. With all these work completed this study had contribution in the following domains:

- GP is an intelligent technique and has been used in different application for optimization purpose. This research work proposed a dynamic block based robust watermarking technique in wavelet domain. GP has been

used to evolve an optimized expression to embed watermark in images using different block sizes in wavelet domain.

- ITFLS based systems have been proposed in different areas successfully. This research described a HVS model based on IT2FLS to tackle the imperceptibility problem efficiently. Using this we obtained best possible watermark weight factor value for each of pixels such that it keep optimum level of imperceptibility.
- Invariant domain for watermarking has been obtained using RT and polynomial transformation. Polynomial transformation based on fractional calculus are introduced and used in watermarking for the first time in this thesis. We also introduced fractional Gaussian field based, fractional variance and threshold. Experimental results confirmed the resulting domain is rotation, translation and scaling invariant.
- We proposed a 3D DIBR image based robust watermarking technique using Multidimensional wavelet transform and IT2FLS to take into account the robustness and imperceptibility properties of watermark. Watermark is embedded in the center image and after wrapping operation the right image and left image are checked for watermark. The experimental results showed that technique is very robust and the BER (BER) is very low.

7.1 Achievements of Objectives

The objectives listed in Chapter 1 has been achieved as described below:

- **To exploit the characteristics of HVS using GP to formulate a perceptual shaping expression for dynamic block approach.**

In Chapter 3 we have designed GP based dynamic block approach in wavelet domain. GP selects suitable watermark strength for each DWT coefficient in each block by using HVS property of Watson perceptual model. The GP assigns optimum watermark weight to embed the watermark imperceptibly. GP function for dynamic block based DWT domain takes into account frequency, luminance sensitivity, and contrast masking. The dynamic size of the block include 4,8,16 and 32. Comparison results showed that our dynamic block based technique is approximately 5%, and 23% more robust than the other two compared techniques.

➤ **To design /propose a new invariant domain for watermarking.**

In chapter 4 we proposed RT based invariant watermarking technique. We explored the invariance properties of the RT especially against rotation, translation and scaling attacks. Furthermore, we incorporated LPM to improve its invariance against rotation attack. For this, we created a geometric invariant domain using RT and LPM. This new invariant domain eliminates synchronization step and is very robust against most of the image processing attacks. Additionally, to improve imperceptibility we used IT2FLS to calculate the watermark weight factor for each of the selected Riesz coefficients. This method is highly practical as it qualifies blind watermark detection.

➤ **To propose a new polynomial transformation based invariant domain for watermarking.**

Our next contribution lies in exploring the Fractional sinc and Fractional Heaviside function for watermarking domain. We tried to exploit the Fractional sinc and Fractional Heaviside function properties for balancing the robustness and imperceptibility properties of watermarking. Furthermore, we also proposed a fractional rotation expression to

achieve rotation robustness. Moreover, we also proposed fractional Gaussian based watermark detection.

➤ **To propose a robust watermarking technique for 2D plus depth images /DIBR 3D images.**

An initial study on 3D DIBR image watermarking was made. We embedded the watermark in the center image and used the depth value of the depth image to select the coefficients for watermark embedding. Furthermore, we proposed a 3D DIBR image based robust watermarking technique using Multidimensional wavelet transform and IT2FLS to take into account the robustness and imperceptibility properties of watermark. The watermark is embedded in the center image and after wrapping operation the right image and left image are checked for watermark. The experimental results showed that proposed technique embedded watermark with least distortion and it is robust to JPEG compression, depth image alteration, Gaussian noise and rotation attacks. Moreover, the BER of the extracted watermark approaches to 0.

7.2 Future Work

Although we have achieved considerable robustness especially against RST attack, and explored new invariant domain, a few possible extensions of this work are identified:

- The geometric invariant domain using RT in chapter 4 has invariance against the rotation attack, but it is limited up to 5 degrees. Future work will look into different ways to improve its variance against more severe rotation attacks.
- For polynomial based watermarking discussed in chapter 5, more research and analysis are needed to explore the properties of these functions for different watermarking scenarios.

REFERENCES

- Abbasi, Almas, & Woo, Chaw Seng. (2012). Robust Image Watermarking Using Genetic Programming. *Journal of Software & Systems Development*, 2012, 1-9.
- Akhbari, B., Ghaemmaghan-Ii, S., & Ieee. (2006). Watermarking of still images in wavelet domain based on entropy masking model *Tencon 2005 - 2005 IEEE Region 10 Conference, Vols 1-5* (pp. 2213-2218). New York: IEEE.
- Almas Abbasi, Woo Chaw Seng. (2013, March 30-31). *Interval Type- 2 Fuzzy logic based Watermarking technique in Discrete Wavelet Domain*. Paper presented at the 2013 International Conference on Emerging Trends in Computer Science & Information Technology (ICETCSIT- 2013), Kuala Lumpur, Malaysia.
- Abbasi, Almas, Woo, Chaw Seng, & Shamshirband, Shahaboddin. (2015). Robust image watermarking based on Riesz transformation and IT2FLS. *Measurement*, 74, 116-129.
- Aslantas, Veysel. (2008). A singular-value decomposition-based image watermarking using genetic algorithm. *AEU-International Journal of Electronics and Communications*, 62(5), 386-394.
- Banzhaf, Wolfgang, Nordin, Peter, Keller, Robert E, & Francone, Frank D. (1998). *Genetic programming: an introduction* (Vol. 1): Morgan Kaufmann San Francisco.
- Barni, Mauro, & Bartolini, Franco. (2004). *Watermarking systems engineering: enabling digital assets security and other applications*: CRC Press.
- Barni, Mauro, Bartolini, Franco, & Piva, Alessandro. (2001). Improved wavelet-based watermarking through pixel-wise masking. *Image Processing, IEEE Transactions on*, 10(5), 783-791.

- Bas, Patrick, Chassery, J-M, & Macq, Benoit. (2002). Geometrically invariant watermarking using feature points. *Image Processing, IEEE Transactions on*, 11(9), 1014-1028.
- Belkacem, S., Dibi, Z., Bouridane, A., & Ieee. (2007). *A masking model of HVS for image watermarking in the DCT domain*. New York: IEEE.
- Bhatnagar, Gaurav, Kumar, Sanjeev, Raman, Balasubramanian, & Sukavanam, Nagarajan. (2009). Stereo image coding via digital watermarking. *Journal of Electronic Imaging*, 18(3), 033012-033012-033019.
- Bracewell, Ronald Newbold, & Bracewell, RN. (1986). *The Fourier transform and its applications* (Vol. 31999): McGraw-Hill New York.
- Castro, Juan R, Castillo, Oscar, & Melin, Patricia. (2007). *An interval type-2 fuzzy logic toolbox for control applications*. Paper presented at the Fuzzy Systems Conference, 2007. FUZZ-IEEE 2007. IEEE International.
- Chammem, Afef, Mitrea, Mihai, & Prêteux, Françoise. (2011). *DWT-based stereoscopic image watermarking*. Paper presented at the IS&T/SPIE Electronic Imaging.
- Chenouard, Nicolas, & Unser, Michael. (2011). *3D steerable wavelets and monogenic analysis for bioimaging*. Paper presented at the Biomedical Imaging: From Nano to Macro, 2011 IEEE International Symposium on.
- Darmstaedter, Vincent, Delaigle, J-F, Nicholson, Didier, & Macq, Benoit. (1998). A block based watermarking technique for MPEG2 signals: Optimization and validation on real digital TV distribution links *Multimedia Applications, Services and Techniques—ECMAST'98* (pp. 190-206): Springer.
- Dobrić, Vladimir, & Ojeda, Francisco M. (2006). Fractional Brownian fields, duality, and martingales *High dimensional probability* (pp. 77-95): Institute of Mathematical Statistics.

- First, E., & Xiaojun, Qi. (2007, Sept. 16 2007-Oct. 19 2007). *A Composite Approach for Blind Grayscale Logo Watermarking*. Paper presented at the Image Processing, 2007. ICIP 2007. IEEE International Conference on.
- Gerald Schaefer , Michal Stich. (Jun 2004). *UCID—An uncompressed colour imagedatabase*. Paper presented at the Proc. SPIE.
- Ghazy, Rania A, El-Fishawy, Nawal Ahmed, Hadhoud, Mohiy Mohammed, Dessouky, Moawad Ibrahim, & Abd El-Samie, Fathi El-Sayed. (2008). Performance evaluation of block based SVD image watermarking. *Progress In Electromagnetics Research B*, 8, 147-159.
- Grove, Jennifer Van. (2011). The State of Photo Sharing on Twitter. <http://mashable.com/2011/06/02/twitter-photo-sharing-stats/>
- Haijun, LUO, Xingming, SUN, Hengfu, YANG, & Zhihua, XIA. (2011). A robust image watermarking based on image restoration using SIFT. *Radioengineering*, 20(2).
- Hernandez, Juan R, Amado, Martin, & Perez-Gonzalez, Fernando. (2000). DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure. *Image Processing, IEEE Transactions on*, 9(1), 55-68.
- Hsieh, Ming-Shing, Tseng, Din-Chang, & Huang, Yong-Huai. (2001). Hiding digital watermarks using multiresolution wavelet transform. *Industrial Electronics, IEEE Transactions on*, 48(5), 875-882.
- Hu Sheng , YangQuan Chen , TianShuang Qiu. (October 26, 2011). *Fractional processes and fractional-order signal processing: techniques and applications (Signals and Communication Technology)*: Springer; 2012 edition (October 26, 2011).
- Huang, Hsiang-Cheh, Pan, Jeng-Shyang, & Chu, Chi-Ming. (2007). *Optimized copyright protection Systems with Genetic-Based Robust Watermarking*. Paper presented at the Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on.

Hwang, Dong-Choon, Bae, Kyung-hoon, Ko, Jung-Hwan, & Kim, Eun-Soo. (2005). *3D watermarking scheme in stereo vision system*. Paper presented at the Proceedings of SPIE, the International Society for Optical Engineering.

Hwang, Dong Choon, Bae, Kyung Hoon, & Kim, Eun-Soo. (2004). *Stereo image watermarking scheme based on discrete wavelet transform and adaptive disparity estimation*. Paper presented at the Optical Science and Technology, SPIE's 48th Annual Meeting.

Ibrahim, Rabha W. (2013). On generalized fractional differentiator signals. *Discrete Dynamics in Nature and Society*, 2013.

Jalab, Hamid A, & Ibrahim, Rabha W. (2012). Denoising algorithm based on generalized fractional integral operator with two parameters. *Discrete Dynamics in Nature and Society*, 2012.

Keyvanpour, Mohammad-Reza, & Merrikh-Bayat, Farnoosh. (2011). Robust dynamic block-based image watermarking in DWT domain. *Procedia Computer Science*, 3, 238-242.

Khan, Asifullah, Mirza, Anwar M, & Majid, Abdul. (2006). Intelligent perceptual shaping of a digital watermark: Exploiting Characteristics of human visual system. *International Journal of Knowledge-based and Intelligent Engineering Systems*, 10(3), 213-223.

Kim, Hee-Dong, Lee, Ji-Won, Oh, Tae-Woo, & Lee, Heung-Kyu. (2012). Robust DT-CWT watermarking for DIBR 3D images. *Broadcasting, IEEE Transactions on*, 58(4), 533-543.

Kim, Hyung Shin, & Lee, Heung-Kyu. (2003). Invariant image watermark using Zernike moments. *Circuits and Systems for Video Technology, IEEE Transactions on*, 13(8), 766-775.

Koza, John R. (1992). *Genetic programming: on the programming of computers by means of natural selection* (Vol. 1): MIT press.

Krishnamoorthi, R.; Malarchelvi, P. D. Sheba Kezia. (April 2009). Image Adaptive Watermarking with Visual Model in Orthogonal Polynomials based Transformation Domain. *International Journal of Signal Processing*; 2009, Vol. 5 Issue 2, p146.

Kundur, Deepa, & Hatzinakos, Dimitrios. (1998). *Digital watermarking using multiresolution wavelet decomposition*. Paper presented at the Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on.

Kutter, Martin, & Petitcolas, Fabien AP. (1999). *Fair benchmark for image watermarking systems*. Paper presented at the Electronic Imaging'99.

Le, L., Krishnan, S., & Ghoraani, B. (2006, 9-12 July 2006). *Discrete polynomial transform for digital Image watermarking Application*. Paper presented at the Multimedia and Expo, 2006 IEEE International Conference on.

Legge, Gordon E, & Foley, John M. (1980). Contrast masking in human vision. *JOSA*, 70(12), 1458-1471.

Leung, Lau Wai, King, Bruce, & Vohora, Vijay. (2001). *Comparison of image data fusion techniques using entropy and INI*. Paper presented at the Paper presented at the 22nd Asian Conference on Remote Sensing.

Li, Jingbing, Bai, Yong, Du, Wencai, & Chen, Yen-wei. (2011). *3D DWT-DCT based multiple watermarks for medical volume data robust to geometrical attacks*. Paper presented at the Electronics, Communications and Control (ICECC), 2011 International Conference on.

Li, Li, Xu, He-Huan, Chang, Chin-Chen, & Ma, Ying-Ying. (2011). A novel image watermarking in redistributed invariant wavelet domain. *Journal of Systems and Software*, 84(6), 923-929.

- Lin, Ching-Yung, Wu, Min, Bloom, Jeffrey A, Cox, Ingemar J, Miller, Matthew L, & Lui, Yui Man. (2001). Rotation, scale, and translation resilient watermarking for images. *Image Processing, IEEE Transactions on*, 10(5), 767-782.
- Lin, Wei-Hung, Wang, Yuh-Rau, Horng, Shi-Jinn, Kao, Tzong-Wann, & Pan, Yi. (2009). A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*, 36(9), 11509-11516.
- Lin, Yu-Hsun, & Wu, Ja-Ling. (2011). A digital blind watermarking for depth-image-based rendering 3D images. *Broadcasting, IEEE Transactions on*, 57(2), 602-611.
- Liu, Zhen, Karam, Lina J, & Watson, Andrew B. (2006). JPEG2000 encoding with perceptual distortion control. *Image Processing, IEEE Transactions on*, 15(7), 1763-1778.
- Maintz, JBA. (2002). Digital and medical image processing. *Lecture Notes, Utrecht University*.
- Mendel, Jerry M. (2001). Uncertain rule-based fuzzy logic system: introduction and new directions.
- Motwani, Mukesh C, & Harris Jr, Frederick C. (2009). *Fuzzy Perceptual Watermarking For Ownership Verification*. Paper presented at the IPCV.
- Nachmias, Jacob, & Sansbury, Richard V. (1974). Grating contrast: discrimination may be better than detection. *Vision research*, 14(10), 1039-1042.
- Nelson, James DB, & Kingsbury, Nick G. (2011). Enhanced shift and scale tolerance for rotation invariant polar matching with dual-tree wavelets. *Image Processing, IEEE Transactions on*, 20(3), 814-821.

- Nikolaidis, Nikos, & Pitas, Ioannis. (1998). Robust image watermarking in the spatial domain. *Signal processing*, 66(3), 385-403.
- Oueslati, Sameh, Cherif, Adnane, & Solaiman, Basel. A Fuzzy Watermarking Approach Based on the Human Visual System. *International Journal Of Image Processing (IJIP)*, 4(3), 218.
- Pan, Jeng-Shyang, Huang, Hsiang-Cheh, & Jain, Lakhmi C. (2004). *Intelligent Watermarking Techniques (Innovative Intelligence)*: World Scientific Press.
- Peli, Eli. (1990). Contrast in complex images. *JOSA A*, 7(10), 2032-2040.
- Peng, Fei, Li, Xiaolong, & Yang, Bin. (2012). Adaptive reversible data hiding scheme based on integer transform. *Signal Processing*, 92(1), 54-62.
- Pham, Viet Quoc, Miyaki, Takashi, Yamasaki, Toshihiko, & Aizawa, Kiyoharu. (2007). *Geometrically invariant object-based watermarking using SIFT feature*. Paper presented at the Image Processing, 2007. ICIP 2007. IEEE International Conference on.
- Piva, Alessandro, Barni, Mauro, Bartolini, Franco, & Cappellini, Vito. (1997). *DCT-based watermark recovering without resorting to the uncorrupted original image*. Paper presented at the Image Processing, 1997. Proceedings., International Conference on.
- Podilchuk, Christine I, & Delp, Edward J. (2001). Digital watermarking: algorithms and applications. *Signal Processing Magazine, IEEE*, 18(4), 33-46.
- Podilchuk, Christine I, & Zeng, Wenjun. (1998). Image-adaptive watermarking using visual models. *Selected Areas in Communications, IEEE Journal on*, 16(4), 525-539.

- Podlubny, Igor. (1999). *Fractional Differential Equations*: Academic Press, San Diego - New York - London.
- Ruanaidh, Joseph JK, & Pun, Thierry. (1998). Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal processing*, 66(3), 303-317.
- Shelby Pereira, Sviatoslav Voloshynovskiy, Maribel Madueño, Stéphane Marchand-Maillet and Thierry Pun. (2001, April 2001). *Second generation benchmarking and application oriented evaluation*. Paper presented at the Information Hiding Workshop III, Pittsburgh, PA, USA
- Shen, Hong, & Chen, Bo. (2012). From single watermark to dual watermark: A new approach for image watermarking. *Computers & Electrical Engineering*, 38(5), 1310-1324.
- Shi, Hailiang, Wang, Nan, Wen, Zihui, Wang, Yue, Zhao, Huiping, & Yang, Yanmin. (2012). *An RST invariant image watermarking scheme using DWT-SVD*. Paper presented at the Instrumentation & Measurement, Sensor Network and Automation (IMSNA), 2012 International Symposium on.
- Smolic, Aljoscha, Mueller, Karsten, Stefanoski, Nikolce, Ostermann, Joern, Gotchev, Atanas, Akar, Gözde B, . . . Koz, Alper. (2007). Coding algorithms for 3DTV—a survey. *Circuits and Systems for Video Technology, IEEE Transactions on*, 17(11), 1606-1621.
- Tripathy, Malay Ranjan, Sachdeva, Kapil, & Talhi, Rachid. (2009). 3D Discrete Wavelet Transform VLSI Architecture for Image Processing. *PIERS Proceedings, Department of Electronics and Communication Engineering Jind Institute of Engineering and Technology, Jind, Haryana, India, Moscow, Russia*.
- Unser, Michael, & Van De Ville, Dimitri. (2010). Wavelet steerability and the higher-order Riesz transform. *Image Processing, IEEE Transactions on*, 19(3), 636-652.
- Urvoy, M., Goudia, D., & Autrusseau, F. (2014). Perceptual DFT Watermarking With Improved Detection and Robustness to Geometrical Distortions. *Ieee*

Transactions on Information Forensics and Security, 9(7), 1108-1119. doi: 10.1109/tifs.2014.2322497

Usman, Imran, & Khan, Asifullah. (2010). BCH coding and intelligent watermark embedding: employing both frequency and strength selection. *Applied Soft Computing*, 10(1), 332-343.

van der Veen, Michiel, Lemma, Aweke, Celik, Mehmet, & Katzenbeisser, Stefan. (2007). Forensic Watermarking in Digital Rights Management *Security, Privacy, and Trust in Modern Data Management* (pp. 287-302): Springer.

Voloshynovskiy, Sviatoslav, Herrigel, Alexander, Baumgaertner, Nazanin, & Pun, Thierry. (2000). *A stochastic approach to content adaptive digital image watermarking*. Paper presented at the Information Hiding.

Wang, Shen, Cui, Chen, & Niu, Xiamu. (2014). Watermarking for DIBR 3D images based on SIFT feature points. *Measurement*, 48, 54-62.

Wang, Zhou, Bovik, Alan C, Sheikh, Hamid R, & Simoncelli, Eero P. (2004). Image quality assessment: from error visibility to structural similarity. *Image Processing, IEEE Transactions on*, 13(4), 600-612.

Weisstein, Eric. (2014a). Delta Function. <http://mathworld.wolfram.com/DeltaFunction.html>

Weisstein, Eric. (2014b). Sinc Function. Retrieved from Wolfram Mathworld website: <http://mathworld.wolfram.com/SincFunction.html>

Wolfgang, R. B., & Delp, E. J. (1996, 16-19 Sep 1996). *A watermark for digital images*. Paper presented at the Image Processing, 1996. Proceedings., International Conference on.

- Woo, Chaw-Seng, Du, Jiang, & Pham, Binh. (2005). *Performance factors analysis of a wavelet-based watermarking method*. Paper presented at the Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44.
- Woo, Chaw-Seng, Du, Jiang, & Pham, Binh. (2006). Geometric invariant domain for image watermarking *Digital Watermarking* (pp. 294-307): Springer.
- Yang, Shouyuan, Song, Zhanjie, Fang, Zhijun, & Yang, Jucheng. (2010). A novel affine attack robust blind watermarking algorithm. *Procedia Engineering*, 7, 239-246.
- Yu, Yanwei, Ling, Hefei, Zou, Fuhao, Lu, Zhengding, & Wang, Liyun. (2012). Robust localized image watermarking based on invariant regions. *Digital Signal Processing*, 22(1), 170-180.
- Yuan, Xiao-Chen, & Pun, Chi-Man. (2012). *A geometric invariant digital image Watermarking Scheme Based on Robust Feature Detector and Local Zernike Moments*. Paper presented at the Computer Graphics, Imaging and Visualization (CGIV), 2012 Ninth International Conference on.
- Zhang, Liang, & Tam, Wa James. (2005). Stereoscopic image generation based on depth images for 3D TV. *Broadcasting, IEEE Transactions on*, 51(2), 191-199.
- Zhao, Yao, Ni, RongRong, & Zhu, ZhenFeng. (2012). RST transforms resistant image watermarking based on centroid and sector-shaped partition. *Science China Information Sciences*, 55(3), 650-662.
- Zheng, Dong, Liu, Yan, Zhao, Jiying, & Saddik, Abdulmotaleb El. (2007). A survey of RST invariant image watermarking algorithms. *ACM Computing Surveys (CSUR)*, 39(2), 5.

List of Publications and Papers Presented

1. Almas Abbasi, Woo Chaw Seng, "Interval Type- 2 Fuzzy logic based Watermarking technique in Discrete Wavelet Domain", 2013 International Conference on Emerging Trends in Computer Science & Information Technology (ICETCSIT- 2013), Kuala Lumpur, Malaysia, March 30-31, 2013.(Kaulalampur, ISBN:9788175371217).
2. Almas Abbasi, Chaw Seng Woo, Rabha Waell Ibrahim, Saeed Islam, "Invariant Domain Watermarking Using Heaviside Function of Order Alpha and Fractional Gaussian Field", PLoS One. 2015 Apr 17; 10(4):e0123427. doi: 10.1371/journal.pone.0123427. eCollection 2015.(Q1) (ISI-Cited Publication).
3. Almas Abbasi, Woo Chaw Seng, Ahmad Imran Shafiq, "Multi Block based Image Watermarking in Wavelet Domain Using Genetic Programming", International Arab Journal OF Information Technology, Vol.11, No.6, pp. 582-589, NOV 2014, ISSN: 1683-3198 (Q4) (ISI-Cited Publication).
4. Almas Abbasi, Chaw Seng Woo, Shahaboddin Shamshirband, "Robust image watermarking based on Riesz transformation and IT2FLS", Measurement, Volume 74, October 2015, Pages 116-129, ISSN 0263-2241, (Q1) (ISI-Cited Publication).
<http://www.sciencedirect.com/science/article/pii/S0263224115003206>.
5. Almas Abbasi, Woo Chaw Seng, "Fuzzy- Logic and Multi-Dimensional Wavelet Transform based Robust Watermarking for DIBR 3D Images". Submitted to ISI Journal.

6. Almas Abbasi, Rabha Ibrahim, Woo Chaw Seng, “Robust watermarking techniques using fractional Sinc transformation”. Submitted to ISI Journal.

University of Malaya